



One Identity Active Roles

User Guide

Copyright 2022 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

 **WARNING:** A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

Active Roles User Guide
Updated - April 2022
Version - 7.5.3

Contents

Introduction	10
Getting Started	11
Starting the Active Roles console	11
MMC interface access management	11
Getting and using help	12
User Interface overview	13
Console tree	13
Details pane	14
Advanced pane	14
Active Roles Security and Links	15
Active Roles Policy	15
Native Security	15
Member Of, Members	16
View mode	16
Controlled objects	16
Using Managed Units	17
Setting up filter	17
Steps for sorting and filtering lists in the details pane	18
Finding objects	19
Steps for searching for a user, contact, or group	19
Steps for searching for a computer	20
Steps for searching for an Organizational Unit	21
Steps for using advanced search options	21
Steps for building a custom search	22
LDAP syntax	22
Search filter format	23
Operators	23
Wildcards	24
Special characters	24
Getting policy-related information	25
One Identity Starling Two-factor Authentication for Active Roles	27

Prerequisites to configure One Identity Starling	27
Logging in to MMC interface through 2FA authentication	28
User or Service Account Management	29
About user accounts	29
User account management tasks	29
Creating a user account	30
Steps for creating a user account	31
Steps for finding a user account	31
Finding a user account	32
Steps for finding a user account	32
Copying a user account	33
Steps for copying a user account	33
Modifying user account properties	34
Steps for modifying user account properties	36
Renaming a user account	36
Steps for renaming a user account	37
Disabling and enabling a user account	38
Steps for disabling a user account	38
Steps for enabling a disabled user account	38
Resetting user password	39
Steps for resetting a user password	39
Adding user accounts to groups	40
Steps for adding a user account to a group	41
Removing a user account from groups	42
Steps for removing a user account from a group	42
Changing a user's primary group	43
Steps for changing a user's primary group	43
Performing Exchange tasks on a user account	43
Steps for performing Exchange tasks	44
Moving user accounts	44
Steps for moving a user account	45
Exporting and importing user accounts	45
Deleting user accounts	45
Steps for deleting a user account	46
Deprovisioning a user account	46

Steps for deprovisioning a user account	47
Restoring a deprovisioned user account	47
Steps for restoring a deprovisioned user account	48
Managing user certificates	48
Steps for managing user certificates	49
Management of group Managed Service Accounts	50
gMSA management tasks	50
Creating a gMSA	51
Managing properties of a gMSA	52
Searching for gMSA in the directory	52
Disabling or re-enabling a gMSA	52
Group Management	54
About groups	54
Group management tasks	55
Creating a group	55
Steps for creating a group	56
Finding a group	57
Steps for finding a group	57
Steps for finding groups in which a user is a member	58
Copying a group	58
Steps for copying a group	59
Modifying group properties	60
Steps for modifying group properties	62
Changing group type and group scope	62
Steps for changing group scope	63
Steps for converting a group to another group type	64
Renaming a group	64
Steps for renaming a group	65
Assigning a manager over a group	65
Steps for assigning a manager over a group	66
Adding members to a group	67
Steps for adding a member to a group	68
Removing members from a group	69
Steps for removing a member from a group	69
Performing Exchange tasks on a group	70

Steps for performing Exchange tasks	70
Moving groups	71
Steps for moving a group	71
Exporting and importing groups	71
Deleting groups	72
Steps for deleting a group	72
Deprovisioning groups	73
Steps for deprovisioning a group	73
Restoring deprovisioned groups	74
Steps for restoring a deprovisioned group	74
Administering query-based distribution groups	75
Steps for creating a query-based distribution group	76
Administering dynamic (rule-based) groups	77
Using temporal group memberships	78
Adding temporal members	78
Viewing temporal members	79
Rescheduling temporal group memberships	80
Removing temporal members	81
Computer Account Management	82
About computer accounts	82
Computer account management tasks	82
Creating a computer account	83
Steps for creating a computer account	84
Finding a computer account	84
Steps for finding a computer account	84
Modifying computer account properties	85
Steps for modifying computer account properties	87
Disabling and enabling a computer account	87
Steps for disabling a computer account	88
Steps for enabling a disabled computer account	88
Resetting a computer account	88
Adding computer accounts to groups	88
Steps for adding a computer account to a group	90
Removing a computer account from groups	90
Steps for removing a computer account from a group	90

Moving computer accounts	91
Steps for moving a computer account	91
Exporting and importing computer accounts	92
Deleting computer accounts	92
Steps for deleting a computer account	93
Managing a remote computer	93
Using Remote Desktop Connection	94
Viewing BitLocker recovery passwords	94
Steps for viewing BitLocker recovery passwords	95
Organizational Unit Management	97
About Organizational Units	97
Organizational Unit management tasks	97
Creating an Organizational Unit	98
Steps for creating an Organizational Unit	98
Finding an Organizational Unit	98
Steps for finding an Organizational Unit	99
Modifying Organizational Unit properties	99
Steps for modifying Organizational Unit properties	100
Renaming an Organizational Unit	101
Steps for renaming an Organizational Unit	101
Moving an Organizational Unit	101
Steps for moving an Organizational Unit	102
Deleting an Organizational Unit	102
Steps for deleting an Organizational Unit	102
Management of Contacts	104
About contacts	104
Contact management tasks	104
Creating a contact	105
Steps for creating a contact	105
Finding a contact	106
Modifying contact properties	106
Renaming a contact	108
Adding and removing contacts from groups	108
Performing Exchange tasks on a contact	109

Steps for performing Exchange tasks	110
Moving contacts	110
Exporting and importing contacts	110
Deleting contacts	111
Management of Exchange Recipients	112
Creating an Exchange mailbox	112
Steps for creating a user mailbox	113
Steps for creating a room or equipment Mailbox	113
Steps for creating a linked mailbox	114
Steps for creating a shared mailbox	115
Performing Exchange tasks	115
Exchange tasks on user accounts	116
Steps for performing Exchange tasks on a user account	117
Move Mailbox task in Exchange 2013 or later	118
Exchange tasks on groups	119
Steps for performing exchange tasks on groups	120
Exchange tasks on contacts	120
Steps for performing Exchange tasks on contacts	120
Managing Exchange-related properties	121
Exchange General tab	121
Exchange Advanced tab	122
E-mail Addresses tab	123
Mail Flow Settings tab	123
Mailbox Settings tab	124
Mailbox Features tab	125
Calendar Settings tab	126
Resource Information tab	127
Resource Policy	128
Resource Information	129
Resource In-Policy Requests	129
Resource Out-of-Policy Requests	130
Master Account tab	130
Mailbox Sharing tab	130
Managing Unified Messaging users	131
Enable a user for Unified Messaging	131

View or change the properties of a UM-enabled user	135
Reset Unified Messaging PIN for a UM-enabled user	137
Disable Unified Messaging for a user	138
About us	139
Contacting us	139
Technical support resources	139

Introduction

Active Roles (formerly known as ActiveRoles®) is an administrative platform that facilitates administration and provisioning for Active Directory and Exchange. Active Roles enables the organization to develop a flexible administrative structure that suits their needs, while ensuring secure delegation of tasks, reduced workloads, and lower costs.

Active Roles increases the productivity of system administrators and help-desk operators by automating provisioning tasks on directory objects in compliance with corporate administrative policies in corporate Active Directory and Exchange environments. The policy enforcement featured in the product guarantees that every administrative action taken is consistent with corporate security standards, which is a top priority for most organizations.

The Active Roles User Guide is designed for individuals responsible for performing administrative tasks using the Active Roles console (MMC Interface). This document provides information about the Active Roles console user interface, and includes instructions to help delegated administrators and help-desk operators perform day-to-day administrative activities.

The Active Roles User Guide is supplemented with the Active Roles Administration Guide that provides conceptual information about the product, and includes systematic instructions on how to deploy the Active Roles administrative structure.

Getting Started

- [Starting the Active Roles console](#)
- [User Interface overview](#)
- [View mode](#)
- [Using Managed Units](#)
- [Setting up filter](#)
- [Finding objects](#)
- [Getting policy-related information](#)

Starting the Active Roles console

The Active Roles console, also referred to as MMC Interface, is a comprehensive administrative tool for managing Active Directory and Microsoft Exchange. With the Active Roles console, you can easily find directory objects and perform administrative tasks.

To start the Active Roles console

- Depending upon the version of your Windows operating system, click **Active Roles 7.5.3 Console** on the **Apps** page or select **All Programs | One Identity Active Roles 7.5.3 | Active Roles 7.5.3 Console** from the **Start** menu.

i **NOTE:** Normally, the Active Roles console automatically chooses the Administration Service and establishes a connection. If the console cannot connect to the Administration Service or you want to manually select the Administration Service, see “Connecting to the Administration Service” in the Active Roles Administration Guide.

MMC interface access management

On installing Active Roles on a computer, the MMC interface user access setting is not enabled by default, and any user is enabled to log in to the MMC interface. You can use

Configuration Center, to set the Active Roles MMC interface user access.

To manage the MMC interface access

1. On the **Dashboard** page in the **Configuration Settings** main window, in the **MMC Interface Access** area, click **Manage Settings**.
2. On the MMC Interface Access page that opens, in the **Settings** area, click on the **Component** item, and then click **Modify** or double-click on the **Component** item.
3. On the MMC Interface Access wizard that is displayed, select one of the following options:
 - **Allow Console (MMC Interface) access for all users:** Enables user to log in to MMC interface.
 - **Restrict Console (MMC Interface) access for all users:** Selecting this option restricts all non Active Roles Administrators from using the console. All delegated users are affected, however, it does not apply to Active Roles Administrators.
4. Click **OK**.

The MMC Interface Access settings get configured successfully. A message is displayed prompting you to restart the Administrative Service to disconnect the current MMC interface user sessions and for the updated settings to be reflected on the MMC interface.

NOTE:

- The user must be delegated with the **User Interfaces** access rights on the **User Interfaces** container under **Server Configuration** to obtain access to the MMC interface. User Interfaces Access templates that provide the access rights are available as part of the Active Roles built-in Access templates in the **User Interfaces** container.
- For information on delegating Console access to specified users, see [Delegating control to users for accessing MMC interface](#).

Getting and using help

Active Roles Help explains concepts and includes instructions for performing tasks with the product.

You can use the following guidelines to get assistance while you work:

- To access Active Roles Help, click **Help** on the **Action** menu or **Help Topics** on the **Help** menu.
- To view description of a dialog box, click the **Help** button in the dialog box or press F1.

- To view a brief description of a menu command or a toolbar button, point to the command or button. The description is displayed in the status bar at the bottom of the window.

You can print a single Help topic or all Help topics under a selected heading.

To print a single Help topic

1. On the menu bar, click **Help** and then click **Help Topics**.
2. In the left pane of the Help viewer, expand the heading that contains the topic you want to print, and then click the topic.
3. On the Help viewer toolbar, click **Options**, click **Print**, and then click **OK**.

To print all Help topics under a heading

1. On the menu bar, click **Help**, and then click **Help Topics**.
2. In the left pane of the Help viewer, click the heading that contains the topics you want to print.
3. On the Help viewer toolbar, click **Options**, and then click **Print**.
4. In the **Print Topics** dialog box, click **Print the selected heading and all subtopics**, and then click **OK**.

User Interface overview

The Active Roles console window is divided into two panes. The left pane contains the console tree, showing the items that are available in the console. The right pane, known as the details pane, displays information about items you select in the console tree. You can perform most management tasks from this pane using commands on the **Action** menu.

Additional information is displayed in the lower sub-pane of the details pane when you check the **Advanced Details Pane** command on the **View** menu. You can perform management tasks from the lower sub-pane using commands on the **Action** menu.

NOTE: On the title bar of the Active Roles Web Interface, click **Feedback** to provide a product feedback. You are redirected to a new browser that allows you to provide the feedback.

- For Admin site, by default, the feedback option is available.
- For HelpDesk site, navigate to **Customization | Global Settings** and check the Enable user feedback link check-box to enable the feedback option.
- The feedback option is not available for SelfService site.

Console tree

The left pane of the Active Roles console contains the console tree.

The console tree root is labeled **Active Roles**. The name of the Administration Service is shown in square brackets. If you have Advanced view mode selected for Active Roles console display (**View | Mode**), the following folders are shown under the console tree root:

- **Configuration** Contains all Active Roles proprietary objects held in containers with appropriate names.
- **Active Directory** Contains a list of domains registered with Active Roles. In this folder, you can browse domains for directory objects (users, group, computers), and perform management tasks on those objects.
- **AD LDS (ADAM)** Contains a list of AD LDS directory partitions registered with Active Roles. In this folder, you can browse partitions for directory objects (users, group, containers), and perform management tasks on those objects.
- **Applications** Contains a list of applications integrated with Active Roles, such as Reporting, and allows for quick access to those applications.

The console display mode determines which folders are displayed in the console tree. For more information, see [View mode](#) later in this document.

Details pane

When you select an item in the console tree, the details pane changes accordingly. To perform administrative tasks, click items in the details pane and use commands on the **Action** menu. The **Action** menu commands also appear on the shortcut menu that you can access by right-clicking items in the console tree or details pane.

By default, the objects listed in the details pane are sorted in ascending order by object name. You can change the sorting order by clicking a column heading. You can add and remove columns in the details pane using the **Choose Columns** command on the **View** menu.

In the Active Roles console you can apply filters to the details pane in order to search for directory objects. To configure a filter, select a domain and then click **Filter Options** on the **View** menu. It is also possible to find an object in the details pane by typing a few characters. This will select the first item in the sorted column that matches what you typed.

Advanced pane

The advanced pane appears at the bottom of the details pane if you check **Advanced Details Pane** on the **View** menu. You can use the advanced pane to administer an object selected in the console tree or details pane: right-click an existing entry in the list to administer it, or right-click a blank area of the advanced pane to add a new entry.

The advanced pane is composed of a number of tabbed pages. The selected object determines which tabs are displayed. All possible tabs in the advanced pane and their descriptions are as follows:

- **Active Roles Security** Lists Active Roles Access Templates applied to the selected object.
- **Links** Lists the objects to which the selected Access Template is applied.
- **Active Roles Policy** Lists Active Roles Policy Objects applied to the selected object.
- **Native Security** Lists Active Directory permission entries specified for the selected object.
- **Member Of** Lists groups to which the selected object belongs.
- **Members** Lists members of the selected group.

NOTE: The console displays the **Active Roles Security**, **Active Roles Policy**, and **Native Security** tabs for a selected object only if your user account has the **Read Control** right to the selected object.

Depending on the tab you have selected in the advanced pane, the toolbar displays the following buttons to help you work with the entries on the tab.

Active Roles Security and Links

Table 1: Active Roles Security and Links

	Apply additional Access Templates to the selected object.
	Display Access Templates that affect the selected object owing to inheritance.
	Synchronize from Active Roles security to Active Directory security.

Active Roles Policy

Table 2: Active Roles Policy

	Apply additional Policy Objects to the selected object.
	Display Policy Objects that affect the selected object owing to inheritance.

Native Security

Table 3: Native Security

	Display permission entries that are inherited from parent objects.
	Display default permission entries specified by the AD schema.

Member Of, Members

Table 4: Member Of and Members

	Add the selected object to groups.
	Set the group as the primary group for the selected object.

View mode

In the Active Roles console you can choose view mode—Basic, Advanced, or Raw. Changing view mode makes it possible to filter out advanced objects and containers from the display.

Basic mode displays Active Directory objects and Managed Units, and filters out objects and containers related to the Active Roles configuration. Basic mode should normally be used by delegated administrators and help-desk operators.

Advanced mode displays all objects and containers except those reserved for Active Roles internal use. Advanced mode is designed for administrators who are responsible for configuring the system and managing Active Roles proprietary objects.

Raw mode displays all objects and containers defined in the Active Roles namespace. This mode is primarily designed for troubleshooting.

With Raw mode, the console displays all data it receives from the Administration Service. With Basic or Advanced mode, some data is filtered out. For example, the **Configuration** folder is not shown in the console tree with Basic mode. Another example is the **Configuration Container** folder used to display the Active Directory configuration naming context, which is displayed with Raw mode only. In addition, there are some commands and property pages that are only displayed when the console is in Raw mode.

In short, when you choose Raw mode, the snap-in displays everything it is able to display. Otherwise, some items are hidden. Note that changing view mode does not modify any items. Rather, this only shows or hides particular items from the display.

To change view mode, click **Mode** on the **View** menu. In the **View Mode** dialog box, click **Basic Mode**, **Advanced Mode**, or **Raw Mode**.

Controlled objects

The Active Roles console provides for visual indication of the objects to which Access Templates or Policy Objects are linked. The console marks those objects by adding an arrow icon at the lower-left corner of the icon that represents the object in the console tree or details pane. As a result, the icon looks similar to the following image: .

To enable this feature, click **Mark Controlled Objects** on the **View** menu, and select check boxes to specify the category of object to be marked.

Using Managed Units

Active Roles offers these key security and administration elements:

- **Trustees** Users or groups that have permissions to administer users, groups, computers, or other directory objects.
- **Permissions and Roles** Permissions are grouped in Access Templates (roles) to define how a Trustee can manage directory objects.
- **Managed Units** Collections of directory objects delegated to Trustees for administration.

The directory administrator defines which users or groups are designated as Trustees, which roles and permissions are assigned to Trustees, and what objects are included in Managed Units.

Managed Units are used to determine the directory objects that a Trustee can administer. As a Trustee, you can administer Managed Units for which you have assigned permissions. Managed Units containing objects you are authorized to administer are displayed under **Managed Units** in the console tree.

When you select a Managed Unit in the console tree, the details pane displays a list of objects included in that Managed Unit. To administer objects, select them from the list and use the commands on the **Action** menu.

If a Managed Unit includes a container, such as an Organizational Unit, the container is displayed under the Managed Unit in the console tree. When you select a container in the console tree, the details pane lists all child objects and sub-containers held in that container.

Setting up filter

The Active Roles console makes it possible to apply a filter to display only the objects that match the filtering criteria. To apply a filter, select an Active Directory object or container and click the **Filter** button on the toolbar: . This displays the **Filter Options** dialog box where you can set up a filter. After you set up a filter, the filtering criteria immediately take effect on all lists of Active Directory objects in the Active Roles console.

Steps for sorting and filtering lists in the details pane

To sort objects in the details pane

1. Click a column heading to sort by the contents of that column.
2. Click the column heading again to switch between ascending and descending sort order.

To add or remove columns in the details pane

1. On the **View** menu, click **Choose Columns** or **Add/Remove Columns**.
2. Do the following, and then click **OK**:
 - To add a column, in **Available columns**, click the column you want to display, and then click **Add**.
 - To remove a column, in **Displayed columns**, click the column you want to hide, and then click **Remove**.
 - To re-order columns, click a column name in **Displayed columns**, and then click **Move Up** or **Move Down** to change the position of the column.

NOTE: In the advanced details pane, you can add or remove columns from a list in the upper sub-pane or in the lower sub-pane: click the list in the sub-pane you want to modify, and then follow the steps above.

Filter options help you search for particular objects in the details pane. You can view all objects or only objects of selected type, configure the number of items that can be displayed for each folder, or create custom filters using object attributes and LDAP queries.

To select view filter options

1. On the **View** menu, click **Filter Options**.
2. Do one of the following, and then click **OK**:
 - To view all objects, click **Show all types of objects**. With this option, the filter is turned off.
 - To view objects of certain types, click **Show only the following types of objects**, and select check boxes next to the types of objects you want to view.
 - To view objects that match custom filtering criteria, click **Create custom filter**. Then, **Customize** and configure your filtering criteria by using the instructions outlined in [Steps for building a custom search](#).
3. Optionally, in **Maximum number of items displayed per folder**, modify the maximum number of objects that can be displayed in the console. The default maximum number of objects displayed in the console is 2,000 objects.

Finding objects

In the Active Roles console you can search for objects of different types using the **Find** window. To access the **Find** window, right-click a container and click **Find**.

From the **In** list, you can select the container or Managed Unit you want to search. The list includes the container that you selected before activating the **Find** window. To add containers to the list, click **Browse**. From the **Find** list, you can select the type of the objects you want to find.

When you select an object type, the **Find** window changes accordingly. For example, **Users, Contacts, and Groups** searches for users, contacts, or groups using criteria such as user name, a note describing a contact, or the name of a group. In the **Find** list, Active Roles splits the **Users, Contacts, and Groups** category into three, providing the option for a more streamlined search.

By selecting **Custom Search** from the **Find** list, you can build custom search queries using advanced search options:

Using the **Find** window, you can search for any directory objects, such as users, groups, computers, Organizational Units, printers or shared folders. It is also possible to search for Active Roles configuration objects such as Access Templates, Managed Units, and Policy Objects. When you search for Access Templates, Policy Objects or Managed Units and select an appropriate object type from the **Find** list, the relevant container appears in the **In** list.

Once the search has completed, the objects matching the search criteria (search results) are listed at the bottom of the **Find** window. You can quickly find an object in the search results list by typing a few characters. This will select the first name that matches what you typed.

Once you have found the object, you can manage it by right-clicking the entry in the search results list, and then clicking commands on the shortcut menu.

Steps for searching for a user, contact, or group

To search for a user, contact, or group

1. On the **Action** menu, click **Find** to display the **Find** window.
2. In the **Find** box, click one of the following:
 - **Users, Contacts, and Groups**, to find users, groups, and contacts that match your search criteria.
 - **Users**, to find only users that match your search criteria.
 - **Groups**, to find only groups that match your search criteria.
 - **Contacts**, to find only contacts that match your search criteria.

3. In the **In** box, select the domain, container or Managed Unit you want to search, or click **Browse** to locate a domain, container or Managed Unit.
4. Type in a name, a description, or both:
 - In the **Name** box, type the name of the object you want to find.
 - In the **Description** box, type the description of the object you want to find.

You can search using partial search criteria. For example, **B** in the **Name** box will return all objects whose name begins with the letter **B**, such as Backup Operators.
5. Click **Find Now** to start your search.

NOTE:

- You can use the **Advanced** tab for more powerful search options. For details, see [Steps for using advanced search options](#).
- The found users, groups, or contacts are displayed at the bottom of the **Find** window.
- You can manage found users, groups, or contacts directly from the list in the **Find** window: right-click a list item, and then use commands on the shortcut menu to perform management tasks.

Steps for searching for a computer

To search for a computer

1. On the **Action** menu, click **Find** to display the **Find** window.
2. In the **Find** box, click **Computers**.
3. In the **In** box, select the domain, container or Managed Unit you want to search, or click **Browse** to locate a domain, container or Managed Unit.
4. In the **Name** box, type the name of the computer you want to find.

You can search using partial search criteria. For example, **B** in the **Name** box will return all computers whose name begins with the letter **B**.
5. Optionally, in the **Role** box, click one of the following:
 - **Domain Controller**, to find only domain controllers.
 - **Workstations and Servers**, to find only workstations and servers (not domain controllers).
6. Click **Find Now** to start your search.

NOTE:

- You can use the **Advanced** tab for more powerful search options. For details, see [Steps for using advanced search options](#).
- The found computers are displayed at the bottom of the **Find** window.
- You can manage found computer objects directly from the list in the **Find** window: right-click a list item, and then use commands on the shortcut menu to perform management tasks.

Steps for searching for an Organizational Unit

To search for an Organizational Unit

1. On the **Action** menu, click **Find** to display the **Find** window.
2. In the **Find** box, click **Organizational Units**.
3. In the **In** box, select the domain, container or Managed Unit you want to search, or click **Browse** to locate a domain, container or Managed Unit.
4. In the **Name** box, type the name (or a part of the name) of the Organizational Unit you want to find.
5. Click **Find Now** to start your search.

NOTE:

- You can use the **Advanced** tab for more powerful search options. For details, see [Steps for using advanced search options](#).
- The found Organizational Units are displayed at the bottom of the **Find** window.
- You can manage found Organizational Units directly from the list in the **Find** window: right-click a list item, and then use commands on the shortcut menu to perform management tasks.

Steps for using advanced search options

To use advanced search options

1. On the **Action** menu, click **Find** to display the **Find** window.
2. In the **Find** box, click the kind of object for which you want to search.
3. Click the **Advanced** tab.
4. Click the **Field** button, and select the object property you want to query.

5. In **Condition**, click the condition for your search, and then, in **Value**, type a property value, in order to find the objects that have the object property matching the condition-value pair you have specified.
6. Click **Add** to add this search condition to your search.
7. Repeat steps 4 through 6 until you have added all of the desired search conditions.
8. Click one of the following:
 - If you want to find the objects that meet all of the conditions specified, click **AND**.
 - If you want to find the objects that meet any of the conditions specified, click **OR**.
9. Click **Find Now** to start your search. The found objects are displayed at the bottom of the window.

Steps for building a custom search

To build a custom search

1. On the **Action** menu, click **Find** to display the **Find** window.
2. In the **Find** box, click **Custom Search**.
3. In the **In** box, select the domain, container or Managed Unit you want to search, or click **Browse** to locate a domain, container or Managed Unit.
4. Do one of the following:
 - On the **Custom Search** tab, follow Steps 4-9 of the procedure outlined in [Steps for using advanced search options](#).
 - On the **Advanced** tab, specify a search filter using [LDAP syntax](#).
5. Click **Find Now** to start your search.

LDAP syntax

Search filters enable you to define search criteria and provide more efficient and effective searches. The search filters are represented by Unicode strings.

The Active Roles console supports the standard LDAP search filters as defined in RFC2254.

The following table lists some examples of standard LDAP search filters.

Table 5: LDAP search filters

Search filter	Description
(objectClass=*)	All objects

Search filter	Description
<code>(&(objectCategory=person) (objectClass=user) (!cn=andy))</code>	All user objects but "andy"
<code>(sn=sm*)</code>	All objects with a surname that starts with "sm"
<code>(&(objectCategory=person) (objectClass=contact) ((sn=Smith) (sn=Johnson)))</code>	All contacts with a surname equal to "Smith" or "Johnson"

Search filter format

Search filters use one of the following formats:

`<filter>=(<attribute><operator><value>)`

or

`(<operator><filter1><filter2>)`

In this example, `<attribute>` stands for the LDAP display name of the attribute by which you want to search.

Operators

The following table lists some frequently used search filter operators.

Table 6: Operators

Logical Operator	Description
<code>=</code>	Equal to
<code>~=</code>	Approximately equal to
<code><=</code>	Lexicographically less than or equal to
<code>>=</code>	Lexicographically greater than or equal to
<code>&</code>	AND
<code> </code>	OR
<code>!</code>	NOT

Wildcards

You can also add wildcards and conditions to a search filter. The following examples show substrings that can be used to search the directory.

Get all entries:

```
(objectClass=*)
```

Get entries containing "bob" somewhere in the common name:

```
(cn=*bob*)
```

Get entries with a common name greater than or equal to "bob":

```
(cn>= 'bob')
```

Get all users with an e-mail attribute:

```
(&(objectClass=user)(mail=*))
```

Get all user entries with an e-mail attribute and a surname equal to "smith":

```
(&(sn=smith)(objectClass=user)(mail=*))
```

Get all user entries with a common name that starts with "andy", "steve", or "margaret":

```
(&(objectClass=user) | (cn=andy*)(cn=steve)(cn=margaret))
```

Get all entries without an e-mail attribute:

```
(!(mail=*))
```

Special characters

If any of the following special characters must appear in the search filter as literals, they must be replaced by the listed escape sequence.

Table 7: Special characters

ASCII Character	Escape Sequence Substitute
*	\2a
(	\28
)	\29
\	\5c
NUL	\00

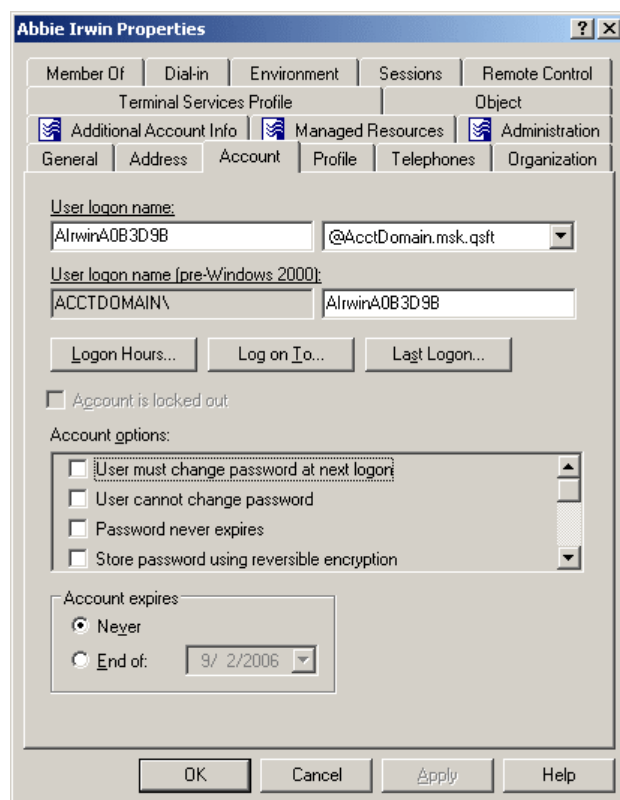
In addition, arbitrary binary data may be represented using the escape sequence syntax by encoding each byte of binary data with the backslash (\) followed by two hexadecimal digits. For example, the four-byte value 0x00000004 is encoded as \00\00\00\04 in a filter string.

Getting policy-related information

In object creation wizards and properties dialog boxes, some property labels may be displayed as hyperlinks. This indicates that Active Roles enforces policy restrictions on the property.

In the following figure, the **User logon name** and **User logon name (pre-Windows 2000)** labels are underlined, which means that these properties are under the control of a certain policy defined with Active Roles.

Figure 1: Getting policy-related information



To examine the policy in detail, you can click the label. For example, if you click **User logon name (pre-Windows 2000)**, the Active Roles console presents you with a window similar to the following figure.

Figure 2: Policy description



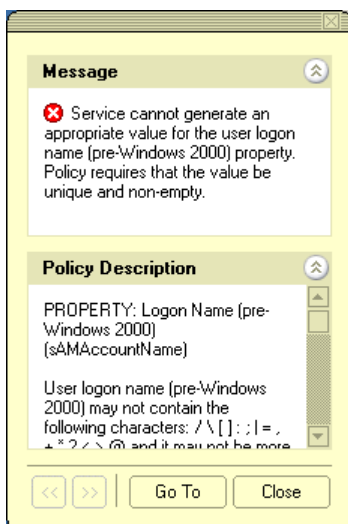
The window may display the following information:

- **Policy Description** Provides a brief description of the policy.
- **Message** Details the problem if the supplied property value violates the policy.

You can click arrows in the lower-left corner to display description of other policies enforced on the given property.

The **Message** section is displayed whenever the specified property value violates the policy. The following figure illustrates the situation where a value has not been supplied for a mandatory property.

Figure 3: Policy violation message



When you click **Go To** in this window, the console moves the pointer to the field that needs to be corrected. You can type or select an appropriate value to correct your input.

One Identity Starling Two-factor Authentication for Active Roles

Since Active Roles manages confidential Active Directory user details in both on-premises and cloud based environments, it is appropriate and safer to have an additional security measure such as the two-factor authentication. Active Roles now supports One Identity's Starling Two-Factor Authentication service.

The Starling Two-factor authentication provides enhanced security by necessitating users to provide two forms of authentication to Active Roles, namely a user name and password combination along with a token response. The token response is collected through an SMS, Phone call, or push notification received on a physical device such as a mobile or any other device other than the browser.

Prerequisites to configure One Identity Starling

Before you configure Starling using the Active Roles Configuration Center, ensure the following:

- Users must have acquired valid Starling Credentials, such as a Starling Organization Admin account or a Collaborator account. For more information on Starling, see the *One Identity Starling User Guide*.
- The computer running Active Roles must have TLS version 1.2 enabled. For more information, see [How to enable TLS 1.2 on clients](#) in the *Microsoft Core infrastructure documentation*.
- The computer running Active Roles must be able to connect directly to the web and reach the following web addresses at a minimum:
 - *.cloud.oneidentity.com
 - *.cloud.oneidentity.eu

NOTE: Additional Microsoft URLs may be required depending on your Starling integration with Azure. For more information, see [KB Article 229909](#) on the One Identity

| Support Portal.

- The Active Roles Administration Service must be running on the computer where you want to configure Starling.
- The Active Roles Administration Service must have a managed domain.
- You must disable **IE Enhanced Security Configuration** to allow the Starling Join process to complete. Once the Starling Join process has completed, you can re-enable this setting.
Follow the steps to disable **IE Enhanced Security Configuration**.

To disable IE Enhanced Security Configuration

1. Open **Server Manager**.
2. On the left pane, select **Local Server**.
3. On the right pane, next to **IE Enhanced Security Configuration**, click **On** and in the popup window, turn **Off** the appropriate connection type (Administrators or Users). If unsure, turn off both connection types.

Logging in to MMC interface through 2FA authentication

When a Starling 2FA enabled user tries to log in to the Active Roles MMC interface, the user is prompted to enter the Starling Two-factor token response. Based on the option selected by the user, the token response is provided through SMS, Phone Call or Push Notifications. After the token is generated the token request options are disabled.

In case the token must be generated again, you need to wait for the minimum notification retry interval for the request options to get enabled. The default value for the notification retry interval period is 30 seconds.

On entering the token response and after successful verification the MMC interface is displayed.

NOTE: Push Notification works only if the Starling App is installed on the device with registered mobile number. The link to install the Starling App will be send to your registered mobile number at the time of registering to Starling.

If the system is kept idle for more than 30 minutes, the 2FA session expires and the MMC console gets disconnected with a session timeout warning.

User or Service Account Management

- [About user accounts](#)
- [User account management tasks](#)
- [Management of group Managed Service Accounts](#)

About user accounts

Active Roles allows you to perform administrative tasks such as create, copy, rename, modify, and delete user accounts in Active Directory. You can also use this tool to unlock accounts, add and remove accounts from groups, and reset user passwords. Active Roles also supports Exchange tasks, such as create, delete, and move user mailboxes.

The following section guides you through the Active Roles console to manage user accounts. You can also perform these tasks using the Active Roles Web Interface.

User account management tasks

This section covers the following tasks:

- [Creating a user account](#)
- [Finding a user account](#)
- [Copying a user account](#)
- [Modifying user account properties](#)
- [Renaming a user account](#)
- [Disabling and enabling a user account](#)
- [Resetting user password](#)
- [Adding user accounts to groups](#)

- [Removing a user account from groups](#)
- [Changing a user's primary group](#)
- [Performing Exchange tasks on a user account](#)
- [Moving user accounts](#)
- [Exporting and importing user accounts](#)
- [Deleting user accounts](#)
- [Deprovisioning a user account](#)
- [Restoring a deprovisioned user account](#)
- [Managing user certificates](#)

Creating a user account

You can create a user account as follows: in the console tree, right-click the container where you want to add the user account, select **New | User**, and then follow the instructions in the wizard.

In the wizard, some property labels may be displayed as hyperlinks. In the following figure, these are **Full name**, **Display name**, **User logon name** and **User logon name (pre-Windows 2000)**. The hyperlink indicates that Active Roles enforces certain policy restrictions on the property. To examine policy details, click the hyperlink: the policy information is displayed (see [Getting policy-related information](#) earlier in this document).

Figure 4: Creating a user account

The policy information is also displayed whenever you supply a property value that violates a policy restriction. The wizard cannot proceed until you enter an acceptable value.

Steps for creating a user account

To create a user account

1. In the console tree, locate and select the folder in which you want to add the user account.
2. Right-click the folder, point to **New** and click **User** to start the New Object - User wizard.
3. Follow the wizard pages to specify properties of the new user account, such as the user first name, last name, full name, display name, logon name, pre-Windows 2000 logon name, password, and Exchange mailbox settings.
4. If you want to set values for additional properties (those for which the wizard pages do not provide data entries), click **Edit Attributes** on the completion page of the wizard.
5. After setting any additional properties for the new user account, click **Finish** on the completion page of the wizard.

NOTE:

- The behavior of the wizard pages may vary depending on the configuration of Active Roles policies. To determine whether a given item on a page is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that certain policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the wizard pages.
- also start the New Object - User wizard by clicking  on the toolbar.
- To create a user account, you can also copy a previously created user account. For more information, see [Copying a user account](#).
- A new user account with the same name as a previously deleted user account does not automatically assume the permissions and group memberships of the previously deleted account because the security ID (SID) for each account is unique. To duplicate a deleted user account, all permissions and memberships must be manually recreated.

Steps for finding a user account

To find a user account

1. On the **Action** menu, click **Find** to display the **Find** window.
2. In the **Find** box, click **Users**.
3. In the **In** box, select the domain, container or Managed Unit you want to search, or click **Browse** to locate a domain, container or Managed Unit.

4. Type in a name, a description, or both:
 - In the **Name** box, type the name (or a part of the name) of the user you want to find.
 - In the **Description** box, type the description (or a part of the description) of the user you want to find.
5. Click **Find Now** to start your search.

NOTE:

- You can manage found user accounts directly from the list in the **Find** window: right-click a list item, and then use commands on the shortcut menu to perform management tasks.
- For more information on how to search for user accounts, see [Steps for searching for a user, contact, or group](#) earlier in this document.
- You can use the **Advanced** tab for more powerful search options. For details, see [Steps for using advanced search options](#) earlier in this document.

Finding a user account

To find a user account, right-click the container you want to search and click **Find**. In the **Find** window, select **Users** from the **Find** list, specify your search criteria, and start the search. In the search results list, you can right-click user accounts and use commands on the shortcut menu to perform management tasks. For more information, see [Finding objects](#) earlier in this document.

Steps for finding a user account

To find a user account

1. On the **Action** menu, click **Find** to display the **Find** window.
2. In the **Find** box, click **Users**.
3. In the **In** box, select the domain, container or Managed Unit you want to search, or click **Browse** to locate a domain, container or Managed Unit.
4. Type in a name, a description, or both:
 - In the **Name** box, type the name (or a part of the name) of the user you want to find.
 - In the **Description** box, type the description (or a part of the description) of the user you want to find.
5. Click **Find Now** to start your search.

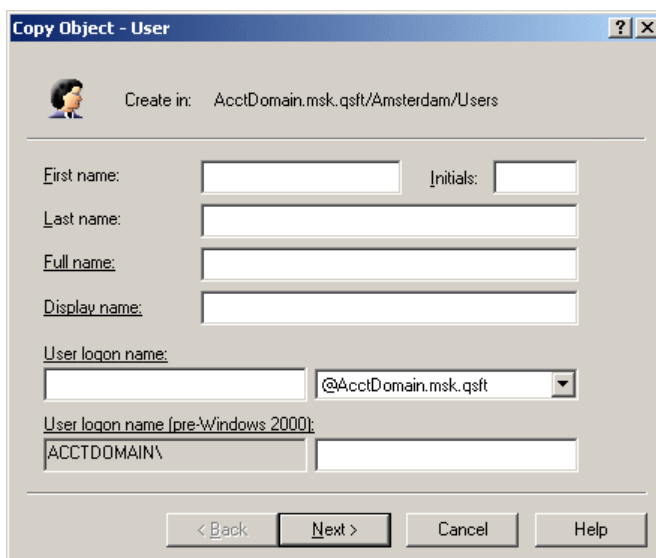
NOTE:

- You can manage found user accounts directly from the list in the **Find** window: right-click a list item, and then use commands on the shortcut menu to perform management tasks.
- For more information on how to search for user accounts, see [Steps for searching for a user, contact, or group](#) earlier in this document.
- You can use the **Advanced** tab for more powerful search options. For details, see [Steps for using advanced search options](#) earlier in this document.

Copying a user account

To create a copy of a user account, right-click the account, click **Copy**, and then follow the instructions in the wizard. The first step of the wizard looks as shown in the following figure.

Figure 5: Copying a user account



The copy of a user account belongs to the same Windows groups as that (original) user account.

Steps for copying a user account

To copy a user account

1. In the console tree, locate and select the folder that contains the user account that you want to copy.

2. In the details pane, right-click the user account you want to copy, and then click **Copy** to start the Copy Object - User wizard.
3. Follow the wizard pages to specify properties for the copy of the user account, such as the user first name, last name, full name, display name, logon name, pre-Windows 2000 logon name, password, and Exchange mailbox settings.
4. If you want to set values for additional properties (those for which the wizard pages do not provide data entries), click **Edit Attributes** on the completion page of the wizard.
5. After setting any additional properties for the copy of the user account, click **Finish** on the completion page of the wizard.

NOTE:

- The behavior of the wizard pages may vary depending on the configuration of Active Roles policies. To determine whether a given item on a page is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the wizard pages.
- By default, some commonly-used properties are carried over to the newly copied user account from the original account. Thus, the group memberships is copied from the original account: if the original account is a member of a given group, the Copy Object - User wizard automatically adds the copy of the account to that group.

Modifying user account properties

To modify user account properties, right-click the account and click **Properties**. You can make changes to user account properties in the **Properties** dialog box, shown in the following figure.

Figure 6: User account properties

The screenshot shows the 'Adrie Fortuyn Properties' dialog box. The 'Object' tab is selected, and the 'Additional Account Info' sub-tab is active. The user's name is 'Adrie Fortuyn', and the description is 'Demo user account for Quick Connect 3.1 Basic Ev'. The telephone number is '+31 20 172-023-39'. The dialog box includes fields for first name, last name, display name, description, office, telephone number, email, and web page, along with buttons for 'Other...' and standard window controls (OK, Cancel, Apply, Help).

In the **Properties** dialog box, some property labels may be displayed as hyperlinks. The hyperlink indicates that Active Roles enforces certain policy restrictions on the property. To examine policy details, click the hyperlink: the policy information is displayed (see [Getting policy-related information](#) earlier in this document).

The policy information is also displayed whenever you supply a property value that violates a policy restriction. Property changes cannot be applied until you enter an acceptable value.

You can use the **Properties** dialog box to view or modify any property of the user account: go to the **Object** tab and click **Advanced Properties**. In the **Advanced Properties** window you can manage all properties, including those that cannot be accessed via the **Properties** dialog box itself.

You can also display the **Advanced Properties** window as follows: right-click the user account and select **All Tasks | Advanced Properties**.

- NOTE:** In the console, you can select multiple user accounts, right-click the selection, click **Properties**, and then modify properties of all the selected accounts collectively via the **Properties** dialog box.

Steps for modifying user account properties

To modify user account properties

1. In the console tree, locate and select the folder that contains the user account that you want to modify.
2. In the details pane, right-click the user account you want to modify, and then click **Properties** to display the **Properties** dialog box for that user account.
3. Use the tabs in the **Properties** dialog box to view or modify properties of the user account.
4. If you want to view or modify additional properties (those for which the tabs in the **Properties** dialog box do not provide data entries), go to the **Object** tab and click **Advanced Properties**.
5. After setting all the properties you want, click **OK**.

i NOTE:

- The behavior of the user interface elements in the **Properties** dialog box may vary depending on the configuration of Active Roles policies. To determine whether a given item on a tab is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the user interface elements.
- To modify properties for multiple user accounts, press and hold down CTRL, and then click each user account. Right-click the selection, and then click **Properties**.
- You can also access the **Advanced Properties** dialog box for a user account as follows: Right-click the user account and select **All Tasks | Advanced Properties**.
- You can use the Find function of Active Roles in order to locate the user account that you want to modify. Once you have found the user account, you can open the **Properties** dialog box for that account as follows: Right-click the user account in the list of search results and click **Properties**.

Renaming a user account

To rename a user account, right-click the account and click **Rename**. Type a new name and press ENTER. This displays the **Rename User** dialog box, shown in the following figure. In the **Rename User** dialog box, you can change the user's first name, last name, display name, and logon name.

Figure 7: Rename User

The 'Rename User' dialog box contains the following fields and values:

- Full name: Adrie Fort
- First name: Adrie
- Last name: Fortuyn
- Display name: Adrie Fortuyn
- User logon name: AFortuynA0B3D9B, @AcctDomain.msk.qsft
- User logon name (pre-Windows 2000): ACCTDOMAIN\, AFortuynA0B3D9B

In the **Rename User** dialog box, hyperlinks are used to indicate the properties controlled by Active Roles policies (see [Getting policy-related information](#) earlier in this document).

Steps for renaming a user account

To rename a user account

1. In the console tree, locate and select the folder that contains the user account.
2. In the details pane, right-click the user account and click **Rename**.
3. Type a new name (or clear the existing name), and then press ENTER to display the **Rename User** dialog box.
4. Use the **Rename User** dialog box to modify (if needed) the naming properties of the user account such as the user full name, first name, last name, display name, and logon name.
5. When finished, click **OK**.

NOTE:

- The behavior of the **Rename User** dialog box may vary depending on the configuration of Active Roles policies. To determine whether a given item in the dialog box is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the dialog box.
- You can use the Find function of Active Roles in order to locate the user account that you want to rename. Once you have found the user account, you can open the **Rename User** dialog box for that account as follows: Right-click the user account in the list of search results, click **Rename**, type a new name, and then press ENTER.

Disabling and enabling a user account

A user account can be disabled as a security measure to prevent a particular user from logging on, instead of deleting the user account.

To disable a user account, right-click the account and click **Disable Account**. To enable a user account, right-click a disabled account and click **Enable Account**. The **Enable Account** command only appears on disabled accounts. Disabled user accounts are marked with the following icon: 

Steps for disabling a user account

To disable a user account

1. In the console tree, locate and select the folder that contains the user account.
2. In the details pane, right-click the user account and click **Disable Account**.

NOTE:

- To prevent particular users from logging on for security reasons, the administrator can disable user accounts instead of deleting user accounts.
- The **Disable Account** command is displayed if the account is enabled and thus can be used for logon; otherwise, the **Enable Account** command is displayed on the menu. By using the **Enable Account** command the administrator can change the status of the disabled account so as to allow the user to log on with that account.
- You can use the Find function of Active Roles in order to locate the user account you want to disable. Once you have found the user account, you can disable it as follows: Right-click the user account in the list of search results and click **Disable Account**.
- Since the Copy function ensures that the copy of a user account belongs to the same groups as the original user account, the administrator can create a disabled user account that belongs to certain groups, and then make copies of that account in order to simplify the creation of user accounts with common group memberships.

Steps for enabling a disabled user account

To enable a disabled user account

1. In the console tree, locate and select the folder that contains the user account.
2. In the details pane, right-click the user account and click **Enable Account**.

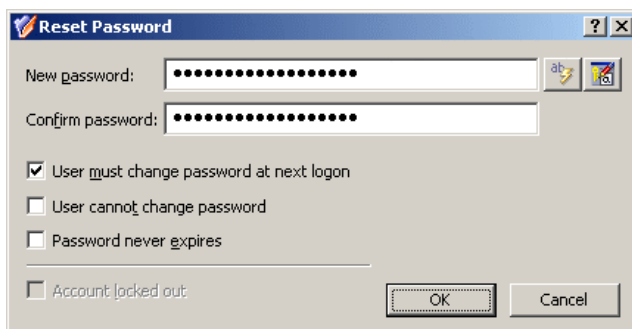
NOTE:

- The **Enable Account** command is displayed if the account is disabled and thus cannot be used for logon; otherwise, the **Disable Account** command is displayed on the menu. To prevent particular users from logging on for security reasons, the administrator can disable user accounts by using the **Disable Account** command.
- You can use the Find function of Active Roles in order to locate the user account you want to enable. Once you have found the user account, you can enable it as follows: Right-click the user account in the list of search results and click **Enable Account**.

Resetting user password

To reset the password for a user account, right-click the account and click **Reset Password**. This displays the **Reset Password** dialog box, shown in the following figure. In the **Reset Password** dialog box, it is possible to generate passwords, set password options, and unlock the account if it is locked out. To generate a password, click the button next to the **New Password** box.

Figure 8: Reset Password



Steps for resetting a user password

To reset a user password

1. In the console tree, locate and select the folder that contains the user account whose password you want to reset.
2. In the details pane, right-click the user account whose password you want to reset, and then click **Reset Password** to display the **Reset Password** dialog box.
3. Type and confirm the password, or click the button next to the **New password** box to have Active Roles generate a password.

4. Select the appropriate check boxes to specify password options. Thus, if you want to require the user to change this password at the next logon process, select the **User must change password at next logon** check box.
5. When finished, click **OK**.

NOTE:

- For an auto-generated password, you can see how to spell out the password: Click the second button next to the **New password** box to display the **Spelling Out** dialog box.
- Services that are authenticated with a user account must be reset if the password for the service's user account is changed.
- You can use the Find function of Active Roles in order to locate the user account whose password you want to reset. Once you have found the user account, you can open the **Reset Password** dialog box for that account as follows: Right-click the user account in the list of search results and click **Reset Password**.

Adding user accounts to groups

To add user accounts to groups, select the accounts, right-click the selection, and click **Add to a group**. This displays the **Select Objects** dialog box where you can select the groups to which you want to add the accounts.

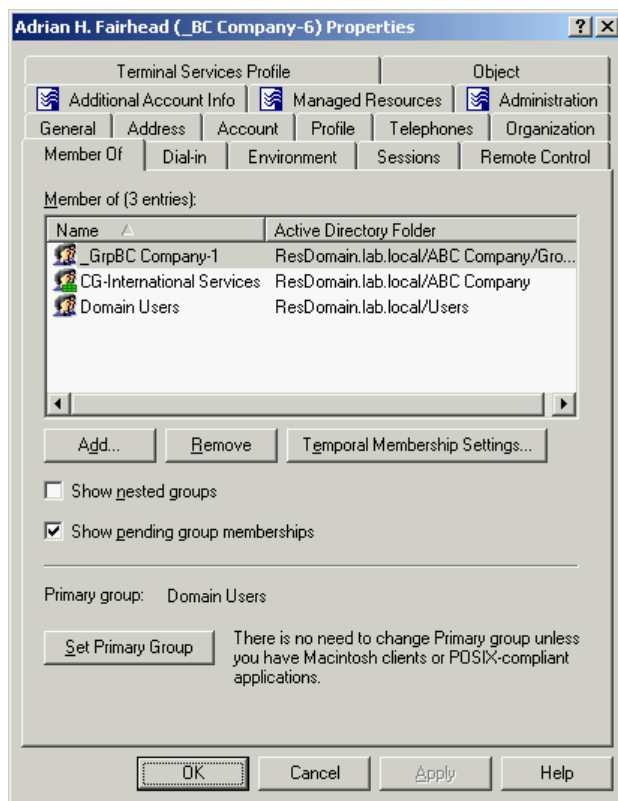
In the **Select Objects** dialog box, you can select groups from the list or type group names, separating them with semicolons. Use the **Check Names** button to verify the names you type. If Active Roles cannot find a group, it prompts you to correct the name.

You can also add a user account to groups by modifying the group membership list on the **Member Of** tab in the **Properties** dialog box. To display the **Properties** dialog box, right-click the user account and click **Properties**.

The **Member Of** tab lists the groups to which the account belongs, as shown in the following figure. If the **Show nested groups** check box is selected, the list also includes the groups to which the account belongs owing to group nesting.

The **Temporal Membership Settings** button can be used to specify the date and time when the user should be added or removed from the selected groups. For more information about this feature, see [Using temporal group memberships](#) later in this document.

Figure 9: Adding user accounts to groups



On the **Member Of** tab, you can manage groups directly from the list of groups. To manage a group, right-click it, and use commands on the shortcut menu.

You can add the user account to groups by clicking **Add** on the **Member Of** tab. This displays the **Select Objects** dialog box, allowing you to select the groups to which you want to add the user account.

- NOTE:** When you select multiple user accounts, the **Member Of** tab lists the groups to which all the selected accounts belong. If one of the accounts does not belong to a given group, that group does not appear in the list.

Steps for adding a user account to a group

To add a user account to a group

1. In the console tree, locate and select the folder that contains the user account.
2. In the details pane, right-click the user account, and then click **Add to a Group**.
3. Use the **Select Objects** dialog box to locate and select the group to which you want to add the user account (you can select more than one group to add the account to).

NOTE:

- You can add multiple user accounts to a group at a time: Select the accounts, right-click the selection, and click **Add to a Group**. To select multiple accounts, press and hold down CTRL, and then click each account.
- You can also add or remove user accounts from groups by using the **Properties** dialog box: Select one or more accounts, right-click the selection, click **Properties**, and go to the **Member Of** tab in the **Properties** dialog box.
- You can use the Find function of Active Roles in order to locate the user accounts you want to add to a certain group. Once you have found the user accounts, you can proceed as follows: Select the accounts in the list of search results, right-click the selection, and click **Add to a Group**.
- By adding a user to a group, you can assign permissions to all of the user accounts in that group and filter Group Policy settings on all accounts in that group.

Removing a user account from groups

To remove a user account from groups, right-click the user account, click **Properties**, and go to the **Member Of** tab. On the **Member Of** tab, select groups from the list and click **Remove**.

Steps for removing a user account from a group

To remove a user account from a group

1. In the console tree, locate and select the folder that contains the user account.
2. In the details pane, right-click the user account, and then click **Properties**.
3. On the **Member Of** tab in the **Properties** dialog box, clear the **Show nested groups** check box, select the group from which you want to remove the user account, and click **Remove**.

NOTE:

- If you have not cleared the **Show nested groups** check box, the list on the **Member Of** tab also includes the groups to which the user account belongs indirectly, that is, because of group nesting. If you select such a group from the list, the **Remove** button is unavailable. A user account can be removed from only those groups of which the account is a direct member.
- The user account cannot be removed from its primary group (Domain Users by default). You first need to change the user's primary group (see [Steps for changing a user's primary group](#) later in this document).

Changing a user's primary group

The user's primary group applies only to users who log on to the network through Services for Macintosh, or to users who run POSIX-compliant applications. If you are not using these services, there is no need to change the primary group from Domain Users, which is the default setting.

To change a user's primary group, right-click the account, click **Properties**, and go to the **Member Of** tab. On the **Member Of** tab, select a group from the list and click the **Set Primary Group** button.

- NOTE:** Only a global or universal security group can be set as the primary group. If you select a group with group scope set to Domain local, or a distribution group, the **Set Primary Group** button is unavailable.

Steps for changing a user's primary group

To change a user's primary group

1. In the console tree, locate and select the folder that contains the user account.
2. In the details pane, right-click the user account, and then click **Properties**.
3. On the **Member Of** tab in the **Properties** dialog box, click the group that you want to set as the user's primary group, and then click **Set Primary Group**.

- NOTE:**
- Primary groups are used exclusively by Macintosh clients and POSIX-compliant applications. Unless you are using these services, there is no need to change the primary group from Domain Users, which is the default value.
 - A user's primary group must be in the same domain as the user's account and the primary group must be either a global or universal security group.
 - Setting the user's primary group membership to a value other than Domain Users may adversely affect performance as all users in the domain are members of Domain Users. If the user's primary group is set to another group, it may cause the group membership to exceed the supported maximum number of members.

Performing Exchange tasks on a user account

To perform Exchange tasks on a user account, right-click the account, click **Exchange Tasks**, and follow the instructions in the Exchange Task Wizard. The Exchange Task Wizard

helps you manage Exchange recipients by providing a set of tasks that apply to the selected account.

For more information, see [Exchange tasks on user accounts](#) later in this document.

Steps for performing Exchange tasks

To perform Exchange tasks on a user account

1. In the console tree, locate and select the folder that contains the user account.
2. In the details pane, right-click the account and click **Exchange Tasks**.
3. Follow the instructions in the Exchange Task Wizard.

i NOTE:

- The Exchange Task Wizard helps you manage Exchange recipients by providing a set of tasks that applies to the selected accounts. For more information, see [Steps for performing Exchange tasks on a user account](#).
- You can perform Exchange tasks on multiple accounts at a time: Select the accounts, right-click the selection, and click **Exchange Tasks** to start the Exchange Task Wizard.
- You can use the Find function of Active Roles in order to locate the user accounts on which you want to perform Exchange tasks. Once you have found the user accounts, you can start the Exchange Task Wizard as follows: Select the accounts in the list of search results, right-click the selection, and click **Exchange Tasks**.

Moving user accounts

To move user accounts to another container, select the accounts, right-click the selection, and then click **Move**. In the **Move** dialog box, select the container to which you want to move the accounts.

- i** NOTE: The console provides the drag-and-drop function for moving objects. To move user accounts, you can drag the selection from the details pane to a destination container in the console tree.

Steps for moving a user account

To move a user account

1. In the console tree, locate and select the folder that contains the user account.
2. In the details pane, right-click the user account and click **Move** to display the **Move** dialog box.
3. In the **Move** dialog box, select the folder to which you want to move the account, and then click **OK**.

i NOTE:

- With Active Roles, user accounts, as well as other directory objects, can only be moved within the same domain. This means that the folder to which you want to move the account must belong to the same domain as the account.
- You can move multiple user accounts at a time: Select the accounts, right-click the selection, and click **Move** to display the **Move** dialog box. To select multiple accounts, press and hold down CTRL, and then click each account.
- You can move user accounts, by using the drag-and-drop feature. To move a selection of objects, drag the selection from the details pane to the destination container in the console tree.
- You can use the Find function of Active Roles in order to locate the user accounts you want to move. Once you have found the user accounts, you can move them as follows: Select the accounts in the list of search results, right-click the selection, and click **Move** to display the **Move** dialog box.

Exporting and importing user accounts

With the Active Roles console, you can export user accounts to an XML file and then import them from that file to populate a container in a different domain. The export and import operations provide a way to relocate user accounts between domains.

To export user accounts, select them, right-click the selection, and select **All Tasks | Export**. In the **Export Objects** dialog box, specify the file where you want to save the data, and click **Save**.

To import user accounts, right-click the container where you want to place the accounts, and then click **Import**. In the **Import Directory Objects** dialog box, select the file to which the user accounts were exported, and click **Open**.

Deleting user accounts

To delete user accounts, select them, right-click the selection, and click **Delete**. Then, click **Yes** to confirm the deletion. If you select multiple user accounts, clicking **Delete** displays

the **Delete Objects** dialog box. To delete all the selected accounts, select the **Apply to all items** check box, and then click **Yes**.

NOTE: Deleting a user account is an irreversible operation. A new user account with the same name as a deleted user account does not automatically assume the permissions and memberships of the deleted account. For this reason, it is advisable to disable rather than delete accounts.

Steps for deleting a user account

To delete a user account

1. In the console tree, locate and select the folder that contains the user account.
2. In the details pane, right-click the user account, and then click **Delete**.

NOTE:

- You can delete multiple user accounts at a time: Select the accounts, right-click the selection, and click **Delete**. To select multiple accounts, press and hold down CTRL, and then click each account.
- Once a user account has been deleted, all permissions and memberships associated with that user account are permanently deleted. Because the security ID (SID) for each account is unique, a new user account with the same name as a previously deleted user account does not automatically assume the permissions and memberships of the previously deleted account. To duplicate a deleted user account, all permissions and memberships must be manually recreated.
- You can deprovision user accounts as follows: Select one or more accounts in the details pane, right-click the selection, and then click **Deprovision**.
- You can use the Find function of Active Roles in order to locate the user accounts you want to delete or deprovision. Once you have found the user accounts, you can proceed as follows: Select the accounts in the list of search results, right-click the selection, and click **Delete** or **Deprovision**.
- When deleting a user account, you may encounter an error message stating that access is denied. A possible cause of this error is that the user account is protected from deletion. To delete a protected user account, you should first go to the **Object** tab in the **Properties** dialog box for that user account, and clear the **Protect object from accidental deletion** check box.

Deprovisioning a user account

Active Roles provides the ability to deprovision rather than delete or only disable user accounts. Deprovisioning a user refers to a set of actions that are performed by Active

in order to prevent the user from logging on to the network and accessing network resources such as the user's mailbox or home folder.

The **Deprovision** command on a user account updates the account as prescribed by the deprovisioning policies. Active Roles comes with a default policy to automate some commonly-used deprovisioning tasks, and allows the administrator to configure and apply additional policies.

Steps for deprovisioning a user account

To deprovision a user account

1. In the console tree, locate and select the folder that contains the user account you want to deprovision.
2. In the details pane, right-click the user account, and then click **Deprovision**.
3. Wait while Active Roles updates the user account.

i NOTE:

- You can deprovision multiple accounts at a time. Select two or more user accounts, right-click the selection, and then click **Deprovision**.
- The **Deprovision** command is also available in the Active Roles Web Interface. When you click the **Deprovision** command, the operation progress and results are displayed. When the operation is completed, Active Roles displays the operation summary, and allows you to examine operation results in detail.
- On a deprovisioned user account, you can use the **Deprovisioning Results** command to view a report that lists the actions taken during the deprovisioning of the account. For each action, the report informs about success or failure of the action. In the event of a failure, the report provides a description of the error situation.
- If a deprovisioned user account needs to be restored (for example, if a user account has been deprovisioned by mistake), the account can be reset to the state it was in before the deprovisioning occurred. This can be accomplished by using the **Undo Deprovisioning** command on the deprovisioned account.

Restoring a deprovisioned user account

Active Roles provides the ability to restore deprovisioned user accounts. The purpose of this operation, referred to as the *Undo Deprovisioning* operation, is to roll back the changes that were made to a user account by the Deprovision operation. When a deprovisioned user account needs to be restored (for example, if a user account has been deprovisioned by mistake), the Undo Deprovisioning operation allows the account to be restored to the state it was in before the changes were made.

Steps for restoring a deprovisioned user account

To restore a deprovisioned user account

1. In the console tree, locate and select the folder that contains the user account you want to restore.
2. In the details pane, right-click the user account, and then click **Undo Deprovisioning**.
3. In the **Password Options** dialog box, choose the options to apply to the password of the restored account, and then click **OK**.

For information about each option, open the **Password Options** dialog box, and then press F1.

4. Wait while Active Roles restores the user account.

When you click the **Undo Deprovisioning** command, the operation progress and results are displayed. When the operation is completed, Active Roles displays the operation summary, and allows you to examine the operation results in detail. You can view a report that lists the actions taken during the restore operation. For each action, the report informs about success or failure of the action. In the event of a failure, the report provides a description of the error situation.

Managing user certificates

You can use Active Roles to add or remove digital (X.509) certificates from user accounts in Active Directory. By adding a certificate to a user account you make the certificate (including the public key associated with the certificate) available to other Active Directory users and to Active Directory-aware applications and services.

The certificates added to Active Directory user accounts are referred to as *published certificates*. Published authentication certificates are used by Active Directory domain controllers during certificate-based authentication. Published encryption certificates can be used to enable access to encrypted contents. For instance, in the case of e-mail encryption, the sender retrieves the recipient's certificate from the Active Directory user account and uses that certificate to encrypt the e-mail message so that the recipient could decrypt the message by using the private key associated with the certificate. A similar process occurs when you want to allow a given user to read an encrypted file. The certificate retrieved from the user account is used to encrypt the file encryption key so that the file encryption key could be obtained by using the private portion of the user's certificate to decrypt the encrypted key material.

To view or change the list of digital certificates for a particular user account, open the **Properties** page for that user account in the Active Roles console or Web Interface and go to the **Published Certificates** tab. From the **Published Certificates** tab, you can perform the following tasks:

- View the list of the certificates published for the user account in Active Directory.
- Examine each of the published certificates in detail.

- Add a certificate from the local certificate store (available in the console only).
- Add a certificate that is saved in a certificate file.
- Remove a certificate from the user account.
- Copy a published certificate to a certificate file.

For each of the certificates that are listed on the **Published Certificates** tab, you can view the following information:

- The purposes that the certificate is intended for (available in the console only).
- The name of the person or company to which the certificate was issued.
- The name of the certification authority that issued the certificate.
- The time period for which the certificate is valid.
- Additional information about the certification authority that issued the certificate, if available.
- The list of all X.509 fields, extensions, and associated properties found in the certificate.
- The hierarchy of certification authorities for the certificate (available in the console only).

Steps for managing user certificates

In the Active Roles console or Web Interface you can use the **Published Certificates** page to view or change the list of digital certificates that are assigned to a given user account in Active Directory. Digital certificates are used for authentication and secure exchanges of information. A certificate securely binds a public encryption key to the entity that holds the corresponding private key. The **Published Certificates** page allows you to add or remove digital certificates from the user account.

To add or remove a certificate for a user account using the Active Roles console

1. Open the **Properties** dialog box for the user account and click the **Published Certificates** tab.
2. Do the following:
 - Click the **Add from Store** button to add a certificate from the local certificate store.
 - Click the **Add from File** button to add a certificate that is saved in a certificate file.
 - Select a certificate from the list on the tab and click the **Remove** button to remove the certificate.

From the **Published Certificates** page in the Active Roles console, you can also view or export any of the certificates listed on that page. Select a certificate from the list and then click the **View Certificate** button to examine the certificate in detail or click the **Copy to File** button to save a copy of the certificate to a file.

To access the **Published Certificates** page in the Web Interface, open the **General Properties** page for the user account and click the **Published Certificates** tab. From the **Published Certificates** page in the Web Interface you can:

- View any of the certificates listed on that page. Click the **View Certificate** button to examine the certificate in detail.
- Add a certificate to the user account from a certificate file. Click the **Add from File** button and select the desired certificate file.
- Remove a certificate from the user account. Select the certificate from the list on the page and click the **Remove** button.
- Save any of the user's certificates to a file. Select the desired certificate from the list on the page and click the **Copy to File** button.

Management of group Managed Service Accounts

Active Roles now allows you to administer group Managed Service Accounts. Introduced in Windows Server 2012, group Managed Service Account (gMSA) is a domain security principal whose password is managed by Windows Server 2012 domain controllers and can be retrieved by multiple systems running Windows Server 2012. Having Windows services use gMSA as their logon account minimizes the administrative overhead by enabling Windows to handle password management for service accounts. Group Managed Service Accounts provide the same functionality as Managed Service Accounts introduced in Windows Server 2008 R2 and extend that functionality over multiple servers.

As you can use a single gMSA on multiple servers, gMSA provides a single identity solution for services running on a server farm. With a service hosted on a server farm, gMSA enables all service instances to use the same logon account (which is a requirement for mutual authentication between the service and the client), while letting Windows change the account's password periodically instead of relying on the administrator to perform that task.

For more information about group Managed Service Accounts, see "Group Managed Service Accounts Overview" at technet.microsoft.com/en-us/library/hh831782.aspx.

gMSA management tasks

The Active Directory domain in which you are going to create and administer group Managed Service Accounts must meet the following requirements:

- The domain has at least one domain controller that runs Windows Server 2012.
- The domain has the KDS Root Key created.

You can create a KDS Root Key by executing the PowerShell command `Add-KDSRootKey` on the Windows Server 2012 based domain controller. See “Create the Key Distribution Services KDS Root Key” at technet.microsoft.com/en-us/library/jj128430.aspx for further details.

NOTE: Exchange operations cannot be performed on the on-premises Exchange Server environment using the gMSA account. For example, Remote mailbox, User mailbox, or Contact.

You can use the Active Roles console to perform the following tasks on group Managed Service Accounts:

- [Creating a gMSA](#)
- [Managing properties of a gMSA](#)
- [Searching for gMSA in the directory](#)
- [Disabling or re-enabling a gMSA](#)

Creating a gMSA

Perform the following steps in the Active Roles console to create a group Service Managed Account (gMSA).

To create a gMSA

1. Right-click the OU or container in which you want to create a gMSA and select **New | Group Managed Service Account**.
2. In the wizard that opens, complete following fields:
 - **Name** Specifies the name of the gMSA in Active Directory.
 - **Description** Specifies a description of the gMSA.
 - **DNS host name** Normally, you should supply the fully qualified domain name of the server on which you are going to use this gMSA. For example, `ITFarm1.domain.com`.
 - **Account name (pre-Windows 2000)** Specifies the legacy logon name of the gMSA (sAMAccountName). Normally, this setting is identical to the name of the gMSA.
 - **Password change interval (days)** Specifies the number of days before a managed password is automatically changed for the gMSA. This setting can be modified only upon account creation. After the gMSA is created, this setting is read-only.
 - **Computers or groups** Specifies the computers on which the gMSA can be used to run services. You can add individual computers to this field, or you can add computers to a security group and then add the group to this field.

Managing properties of a gMSA

For an existing group Managed Service Account (gMSA), perform the following steps in the Active Roles console to view or change the properties of the gMSA.

To view or change the properties of the gMSA

- Right-click the gMSA you want to administer and click **Properties**.

This opens the **Properties** dialog box containing the same fields as the gMSA creation wizard (see [Creating a gMSA](#)) with the only difference that the **Password change interval** field is read-only. In addition, the **Account is disabled** check box on the **Account** page shows whether the gMSA is disabled for logon, and allows you to disable and re-enable the gMSA.

Searching for gMSA in the directory

The Active Roles console allows you to find group Managed Service Accounts that meet your search conditions.

To search for gMSA in the directory

1. Right-click the OU, domain or container in which you want to search for gMSA and click **Find**.
2. In the **Find** window that opens, configure and start your search:
 - a. In the **Find** list, click **Custom Search**.
 - b. Click the **Field** button, and select the **msDS-GroupManagedServiceAccount** object type and the object property to search for.
 - c. Configure and add the desired search condition for the object property you have selected.
 - d. If needed, add more search conditions by repeating Steps b and c.
 - e. Click **Find Now**.

In the list of search results, right-click a gMSA and use the shortcut menu to perform management tasks. For example, you can right-click a gMSA and then click **Properties** to view or change the properties of the gMSA.

Disabling or re-enabling a gMSA

The Active Roles console allows you to disable a gMSA so that the gMSA cannot be used for logon. For a disabled gMSA, you can use the console to re-enable that gMSA.

To disable or re-enable a gMSA

1. Right-click the gMSA you want to administer and click **Properties**.
2. In the **Properties** dialog box, click the **Account** tab, and examine the **Account is disabled** check box:
 - If the check box is not selected, then the gMSA is enabled for logon. You can disable the gMSA by selecting the **Account is disabled** check box.
 - If the check box is selected, then the gMSA is disabled. You can re-enable the gMSA by clearing the **Account is disabled** check box.

Alternatively, you can use the **Disable Account** or **Enable Account** command on the gMSA object to disable or re-enable the gMSA.

Group Management

- [About groups](#)
- [Group management tasks](#)
- [Using temporal group memberships](#)

About groups

Groups are Active Directory objects used to collect users, contacts, computers, and other groups into manageable units. There are three kinds of groups:

- **Security groups** Used to manage user and computer access to shared network resources. When assigning permissions to access resources, administrators assign permissions to security groups rather than to individual users.
- **Distribution groups** Used as e-mail distribution lists. Distribution groups have no security function.
- **Query-Based Distribution groups** Used also as e-mail distribution lists but the difference is that members of such a group are not specified statically. Membership of these groups is built in dynamic manner using LDAP queries.

In this document, security and distribution groups are collectively referred to as *groups*. As for Query-based distribution groups, these are considered a separate category of groups.

Each group has a scope: universal, global, or domain local.

- **Universal** groups can include groups and accounts from any domain in the domain tree or forest, and can be granted permissions in any domain in the domain tree or forest.
- **Global** groups can only include groups and accounts from the domain in which the group is defined. Global groups can be granted permissions in any domain in the forest.
- **Domain local** groups can include groups and accounts from other domains. These groups can only be granted permissions within the domain in which the group is defined.

A group can be a member of another group. This is referred to as *group nesting*. Group nesting increases the number of affected member accounts and thus consolidates group management. Accounts that reside in a group nested within another group are indirect members of the nesting group.

Active Roles provides the facility to perform administrative tasks such as create copy, rename, modify, and delete groups. It can also be used to add and remove members from groups and perform Exchange tasks on groups.

The following section describes how to use the Active Roles console to manage groups. You can also use the Active Roles Web Interface to perform the group management tasks.

Group management tasks

This section covers the following tasks:

- [Creating a group](#)
- [Finding a group](#)
- [Copying a group](#)
- [Modifying group properties](#)
- [Changing group type and group scope](#)
- [Renaming a group](#)
- [Assigning a manager over a group](#)
- [Adding members to a group](#)
- [Removing members from a group](#)
- [Performing Exchange tasks on a group](#)
- [Moving groups](#)
- [Exporting and importing groups](#)
- [Deleting groups](#)
- [Deprovisioning groups](#)
- [Restoring deprovisioned groups](#)
- [Administering query-based distribution groups](#)
- [Administering dynamic \(rule-based\) groups](#)

Creating a group

You can create a group as follows: in the console tree, right-click the container where you want to add the group, select **New | Group**, and then follow the instructions in the wizard.

In the wizard, some property labels may be displayed as hyperlinks. In the following figure, these are **Group name** and **Group name (pre-Windows 2000)**. The hyperlink indicates that Active Roles enforces certain policy restrictions on the property. To examine policy details, click the hyperlink: the policy information is displayed (see [Getting policy-related information](#) earlier in this document).

Figure 10: Creating a group

The screenshot shows the 'New Object - Group' wizard. The 'Create in' path is 'ResDomain.msk.qst/ABC Company/Groups'. The 'Group name' and 'Group name (pre-Windows 2000)' fields are hyperlinked. The 'Description' field is also present. The 'Group scope' section has radio buttons for 'Domain local', 'Global' (selected), and 'Universal'. The 'Group type' section has radio buttons for 'Security' (selected) and 'Distribution'. The bottom buttons are '< Back', 'Next >', 'Cancel', and 'Help'.

The policy information is also displayed whenever you supply a property value that violates a policy restriction. The wizard cannot proceed until you enter an acceptable value.

Steps for creating a group

To create a group

1. In the console tree, locate and select the folder in which you want to add the group.
2. Right-click the folder, point to **New** and click **Group** to start the New Object - Group wizard.
3. Follow the wizard pages to specify properties of the new group, such as the group name, pre-Windows 2000 group name, description, scope, type, membership list, and Exchange address settings.
4. If you want to set values for additional properties (those for which the wizard pages do not provide data entries), click **Edit Attributes** on the completion page of the wizard.
5. After setting any additional properties for the new group, click **Finish** on the completion page of the wizard.

NOTE:

- The behavior of the wizard pages may vary depending on the configuration of Active Roles policies. To determine whether a given item on a page is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the wizard pages.
- You can also start the New Object - Group wizard by clicking  on the toolbar.
- To create a group, you can also copy a previously created group. For more information, see [Copying a group](#) later in this document.
- A new user account with the same name as a previously deleted user account does not automatically assume the permissions and group memberships of the previously deleted account because the security ID (SID) for each account is unique. To duplicate a deleted user account, all permissions and memberships must be manually recreated.

Finding a group

To find a group, right-click the container you want to search, and click **Find**. In the **Find** window, select **Groups** from the **Find** list, specify your search criteria, and start the search. In the search results list, you can right-click groups and use commands on the shortcut menu to perform management tasks. For more information, see [Finding objects](#) earlier in this document.

Steps for finding a group

To find a group

1. On the **Action** menu, click **Find** to display the **Find** window.
2. In the **Find** box, click **Groups**.
3. In the **In** box, select the domain, container or Managed Unit you want to search, or click **Browse** to locate a domain, container or Managed Unit.
4. Type in a name, a description, or both:
 - In the **Name** box, type the name (or a part of the name) of the group you want to find.
 - In the **Description** box, type the description (or a part of the description) of the group you want to find.
5. Click **Find Now** to start your search.

NOTE:

- You can manage found groups directly from the list in the **Find** window: right-click a list item, and then use commands on the shortcut menu to perform management tasks.
- In the **Find** window, You can use the **Group Type** tab in order to limit your search to groups of certain categories. Select the **Show only groups** check box, select the check boxes specific to the categories of the groups you want to find, and then click **Find Now**. For instance, you can select the **Distribution** check box to search for groups that have the group type set to Distribution, or you can select both the **Global** and **Universal** check boxes to search for groups that have the group scope set to either Global or Universal.
- For more information on how to search for groups, see [Steps for searching for a user, contact, or group](#) earlier in this document.
- You can use the **Advanced** tab for more powerful search options. For details, see [Steps for using advanced search options](#) earlier in this document.

Steps for finding groups in which a user is a member

To find groups in which a user is a member

1. In the console tree, locate and select the folder that contains the user account.
2. In the details pane, right-click the user account, and then click **Properties**.
3. Click the **Member Of** tab.

NOTE:

- The **Member Of** tab for a user displays a list of groups in the domain where the user's account is located. Active Roles does not display groups that reside in trusted domains.
- On the **Member Of** tab, you can select the **Show nested groups** check box in order for the list to also include the groups to which the user belongs because of group nesting.

Copying a group

To create a copy of a group, right-click the group, click **Copy**, and follow the instructions in the wizard. The first step of the wizard looks as shown in the following figure.

Figure 11: Copying a group

The screenshot shows the 'Copy Object - Group' wizard. At the top, it says 'Create in: AcctDomain.msk.qst/Amsterdam/Groups'. Below this are three text input fields: 'Group name:', 'Group name (pre-Windows 2000):', and 'Description:'. Under 'Group scope', there are three radio buttons: 'Domain local', 'Global', and 'Universal'. Under 'Group type', there are two radio buttons: 'Security' and 'Distribution'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

The copy contains the same permission settings as the original group. The Copy Object - Group wizard allows you to modify the membership list of the new group.

Steps for copying a group

To copy a group

1. In the console tree, locate and select the folder that contains the group that you want to copy.
2. In the details pane, right-click the group you want to copy, and then click **Copy** to start the Copy Object - Group wizard.
3. Follow the wizard pages to specify properties of the new group, such as the group name, pre-Windows 2000 name, description, membership list, and Exchange address settings.
4. If you want to set values for additional properties (those for which the wizard pages do not provide data entries), click **Edit Attributes** on the completion page of the wizard.
5. After setting any additional properties for the copy of the group, click **Finish** on the completion page of the wizard.

NOTE:

- The behavior of the wizard pages may vary depending on the configuration of Active Roles policies. To determine whether a given item on a page is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the wizard pages.
- By default, some commonly-used properties are carried over to the newly copied group from the original group. Thus, the group membership list is copied from the original group, and can be modified in the Copy Object - Group wizard.
- The group scope and group type are also copied from the original group, but these properties cannot be modified in the Copy Object - Group wizard. You can change these properties after the copy of the group is created. For instructions, see [Steps for converting a group to another group type](#) and [Steps for changing group scope](#) later in this document.
- You can use the Find function of Active Roles in order to locate the group that you want to copy. Once you have found the group, you can start the Copy Object - Group wizard from the **Find** dialog box: Right-click the group in the list of search results and click **Copy**.

Modifying group properties

To modify group properties, right-click the group and click **Properties**. You can make changes to group properties using the **Properties** dialog box, shown in the following figure.

Figure 12: Modifying group properties

The screenshot shows the 'AMS Sales Properties' dialog box with the 'Object' tab selected. The 'General' sub-tab is active, displaying various group properties. The 'Group name (pre-Windows 2000)' field contains 'AMS SalesA0B3D9B'. The 'Display name' field is empty. The 'Description' field contains 'Demo group for Quick Connect 3.5 Basic Evaluation So'. The 'Resource URL' field is empty with a green arrow button to its right. The 'Keywords' field is empty with a three-dot button to its right. The 'E-mail' field is empty. The 'Group scope' section has three radio buttons: 'Domain local', 'Global' (which is selected), and 'Universal'. The 'Group type' section has two radio buttons: 'Security' (which is selected) and 'Distribution'. At the bottom, there is a 'Notes' text area and four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

In the **Properties** dialog box, some property labels may be displayed as hyperlinks. The hyperlink indicates that Active Roles enforces certain policy restrictions on the property. To examine policy details, click the hyperlink: the policy information is displayed (see [Getting policy-related information](#) earlier in this document).

The policy information is also displayed whenever you supply a property value that violates a policy restriction. Property changes cannot be applied until you enter an acceptable value.

You can use the **Properties** dialog box to view or modify any property of the group: go to the **Object** tab and click **Advanced Properties**. In the **Advanced Properties** window you can manage all properties, including those that cannot be accessed via the **Properties** dialog box itself.

You can also display the **Advanced Properties** window as follows: right-click the group and select **All Tasks | Advanced Properties**.

- NOTE:** In the console, you can select multiple groups, right-click the selection, click **Properties**, and then modify properties of all the selected groups collectively via the **Properties** dialog box.

Steps for modifying group properties

To modify group properties

1. In the console tree, locate and select the folder that contains the group you want to modify.
2. In the details pane, right-click the group you want to modify, and then click **Properties** to display the **Properties** dialog box for that group.
3. Use the tabs in the **Properties** dialog box to view or modify properties of the group.
4. If you want to view or modify additional properties (those for which the tabs in the **Properties** dialog box do not provide data entries), go to the **Object** tab and click **Advanced Properties**.
5. After setting all the properties you want, click **OK**.

i NOTE:

- The behavior of the user interface elements in the **Properties** dialog box may vary depending on the configuration of Active Roles policies. To determine whether a given item on a tab is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the user interface elements.
- To modify properties for multiple groups, press and hold down CTRL, and then click each group. Right-click the selection, and then click **Properties**.
- You can also access the **Advanced Properties** dialog box for a group as follows: Right-click the group and select **All Tasks | Advanced Properties**.
- You can use the Find function of Active Roles in order to locate the group you want to modify. Once you have found the group, you can open the **Properties** dialog box for that group as follows: Right-click the group in the list of search results and click **Properties**.

Changing group type and group scope

To change group scope or group type, right-click the group, click **Properties**, and go to the **General** tab in the **Properties** dialog box, shown in the following figure. On the **General** tab, click the group type in the **Group type** area or click the group scope under **Group scope**.

Figure 13: Changing group type and group scope

The screenshot shows the 'AMS Sales Properties' dialog box with the 'General' tab selected. The 'Group name (pre-Windows 2000):' field contains 'AMS SalesA0B3D9B'. The 'Display name:' field is empty. The 'Description:' field contains 'group for Quick Connect 3.5 Basic Evaluation Scenario'. The 'Resource URL:' field is empty with a green arrow button to its right. The 'Keywords:' field is empty with a three-dot button to its right. The 'E-mail:' field is empty. Under 'Group scope', the 'Universal' radio button is selected. Under 'Group type', the 'Distribution' radio button is selected. At the bottom, there are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

Steps for changing group scope

To change group scope

1. In the console tree, locate and select the folder that contains the group you want to modify.
2. In the details pane, right-click the group you want to modify, and then click **Properties**.
3. On the **General** tab in the **Properties** dialog box, under **Group scope**, click the group scope you want for this group.

For information about possible scope settings, see [About groups](#) earlier in this document.

NOTE:

The following changes of the group scope are allowed:

- **Global to universal** This is allowed if the group you want to change is not a member of another global group.
- **Domain local to universal** This is allowed if the group you want to change does not have another domain local group as a member.
- **Universal to global** This is allowed if the group you want to change does not have another universal group as a member.
- **Universal to domain local** No restrictions for this operation.

Steps for converting a group to another group type

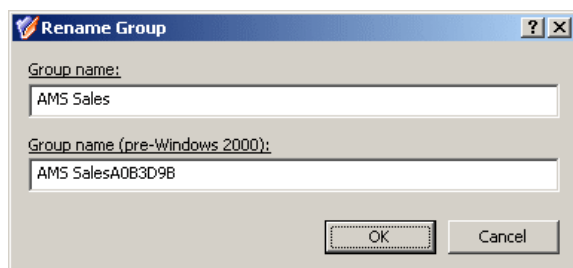
To convert a group to another group type

1. In the console tree, locate and select the folder that contains the group you want to modify.
2. In the details pane, right-click the group you want to modify, and then click **Properties**.
3. On the **General** tab in the **Properties** dialog box, under **Group type**, click the group type you want for this group.

Renaming a group

To rename a group, right-click the group, and then click **Rename**. Type a new name and press ENTER. This displays the **Rename Group** dialog box, shown in the following figure. In the **Rename Group** dialog box, you can change the group name and group name (pre-Windows 2000).

Figure 14: Rename Group



In the **Rename Group** dialog box, hyperlinks are used to indicate the properties controlled by Active Roles policies (see [Getting policy-related information](#) earlier in this document).

Steps for renaming a group

To rename a group

1. In the console tree, locate and select the folder that contains the group.
2. In the details pane, right-click the group and click **Rename**.
3. Type a new name (or clear the existing name), and then press ENTER to display the **Rename Group** dialog box.
4. Use the **Rename Group** dialog box to modify (if needed) the group name and the group name (pre-Windows 2000).
5. When finished, click **OK**.

i NOTE:

- The behavior of the **Rename Group** dialog box may vary depending on the configuration of Active Roles policies. To determine whether a given item in the dialog box is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the dialog box.
- You can use the Find function of Active Roles in order to locate the group you want to rename. Once you have found the group, you can open the **Rename Group** dialog box for that group as follows: Right-click the group in the list of search results, click **Rename**, type a new name, and then press ENTER.

Assigning a manager over a group

To assign a manager over a group, right-click the group, click **Properties**, and go to the **Managed By** tab in the **Properties** dialog box, shown in the following figure. On the **Managed By** tab, click **Change** and select the user or contact to designate as the manager.

Figure 15: Assigning a manager over a group

The screenshot shows the 'AMS Sales Properties' dialog box with the 'Managed By' tab selected. The 'Name' field contains 'AcctDomain.msk.qsft/Amsterdam/Users/Betje Koch' with 'Change...', 'Properties', and 'Clear' buttons below it. A checked checkbox 'Manager can update membership list' is present. Below are fields for 'Office:', 'Street:', 'City:' (containing 'Amsterdam'), 'State/province:', and 'Country/region:'. There are also fields for 'Telephone number:' (containing '+31 20 319-576-39') and 'Fax number:'. The 'Secondary owners' field contains 'Johan Nipius;Marc Beerda' with an ellipsis button. A checkbox 'Secondary owners can update membership list' is unchecked. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

If you select **Manager can update membership list**, the manager can use Active Roles to add and remove members from the group.

It is possible to assign multiple group owners, to load balance the management of the group. To assign additional owners to the group, click the button next to the **Secondary owners** box. Group owners can be given the same rights over the group as the manager. For example, selecting the check box beneath the **Secondary owners** box gives the secondary owners the authority to add or remove members from the group.

It is possible to assign management of the group to another group: you can select a group in the **Select Objects** dialog box that you use to specify the manager or a secondary owner. This enables every member of the group to act as the manager or secondary owner.

Steps for assigning a manager over a group

To assign a manager over a group

1. In the console tree, locate and select the folder that contains the group.
2. In the details pane, right-click the group, and then click **Properties**.
3. On the **Managed By** tab in the **Properties** dialog box, click **Change** under the **Name** box.

4. Use the **Select Objects** dialog box to locate and select the user or contact you want to be responsible for the group - the manager of the group.
5. Optionally, select the **Manager can update membership list** check box in order to authorize the manager to add or remove members from the group.

NOTE:

- To assign additional managers to the group, click the button next to the **Secondary owners** box. Secondary owners can be given the same rights over the group as the manager. For example, selecting the check box beneath the **Secondary owners** box gives the secondary owners the authority to add or remove members from the group.
- You can select a group for the role of the manager or secondary owner. This enables every member of the group to act as the manager or secondary owner.
- You can use the Find function of Active Roles in order to locate the group you want to modify. Once you have found the group, you can open the **Properties** dialog box for that group as follows: Right-click the group in the list of search results and click **Properties**.

Adding members to a group

Depending on its scope, a group may contain members (users, groups, computers, contacts) from anywhere in the forest, or only members from its own domain.

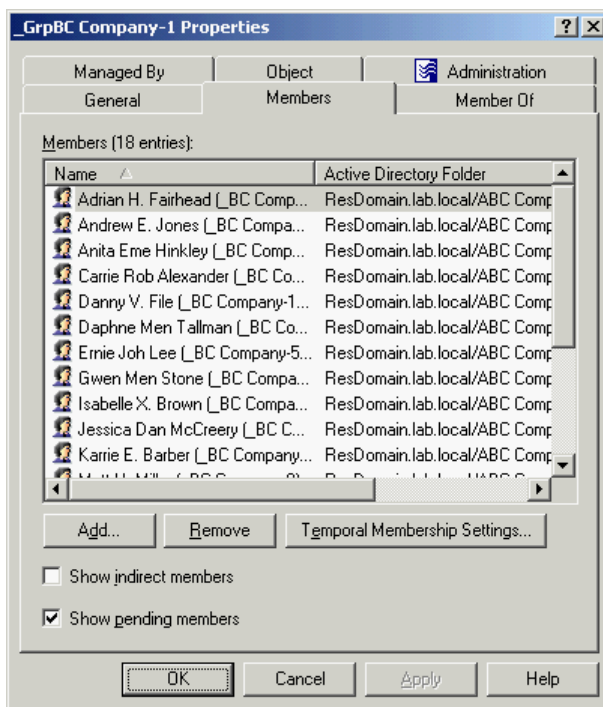
To add members to a group, right-click the group, click **Properties**, and go to the **Members** tab in the **Properties** dialog box. On the **Members** tab, click **Add**. This displays the **Select Objects** dialog box where you can select the objects you want to add to the group.

In the **Select Objects** dialog box, you can select objects from the list or type object names. Use the **Check Names** button to verify the names you type. If Active Roles cannot find an object, it prompts you to correct the name.

The **Members** tab lists objects that belong to the group. If the **Show indirect members** check box is selected, the list also includes the objects that belong to the group because of group nesting.

The **Temporal Membership Settings** button can be used to specify the date and time when the selected members should be added or removed from the group. For more information about this feature, see [Using temporal group memberships](#) later in this document.

Figure 16: Adding members to a group



On the **Members** tab, you can manage user accounts and other objects directly from the list of members. To manage a group member, right-click the member and use commands on the shortcut menu.

NOTE: When you select multiple groups, the **Members** tab lists the objects that belong to each of the selected groups. If a given object does not belong to one of the selected groups, then that object does not appear in the list.

Steps for adding a member to a group

To add a member to a group

1. In the console tree, locate and select the folder that contains the group to which you want to add a member.
2. In the details pane, right-click the group, and then click **Properties**.
3. On the **Members** tab in the **Properties** dialog box, click **Add**.
4. In the **Select Objects** dialog box, type the name of the directory object, such as a user or computer, that you want to add to the group, or select and add the object from the list, and then click **OK**.

NOTE:

- In addition to users and computers, membership in a particular group can include contacts and other groups.
- The **Members** tab displays a list of objects that belong to the group. You can select the **Show indirect members** check box for the **Members** list to also display the objects that belong to the group indirectly (because of group nesting). If that check box is cleared, the **Members** list displays only those objects that were added to the group directly.
- The **Add** button appears on the **Members** tab only if the group is a basic group. For a dynamic group, use the **Membership Rules** tab to populate the group. For details, see [Administering dynamic \(rule-based\) groups](#) later in this document.
- Depending on the scope of a group, the group can hold members from anywhere in the forest or only from its own domain. For more information, see [About groups](#) earlier in this document.

Removing members from a group

To remove members from a group, right-click the group, click **Properties**, and go to the **Members** tab in the **Properties** dialog box. On the **Members** tab, select members from the list and click **Remove**.

Steps for removing a member from a group

To remove a member from a group

1. In the console tree, locate and select the folder that contains the group from which you want to remove a member.
2. In the details pane, right-click the group, and then click **Properties**.
3. On the **Members** tab in the **Properties** dialog box, click the member you want to remove, and then click **Remove**.

NOTE:

- The **Members** tab displays a list of objects that belong to the group. You can select the **Show indirect members** check box for the **Members** list to also display the objects that belong to the group indirectly (because of group nesting). If that check box is cleared, the **Members** list displays only those objects that were added to the group directly.
- With the **Show indirect members** check box selected, the **Members** list also includes the objects that belong to the group indirectly. If you select such an object from the list, the **Remove** button is unavailable. An object can be removed from only those groups of which the object is a direct member.
- The **Remove** button appears on the **Members** tab only if the group is a basic group. For a dynamic group, use the **Membership Rules** tab to add or remove members from the group. For details, see [Administering dynamic \(rule-based\) groups](#) later in this document.

Performing Exchange tasks on a group

To perform Exchange tasks on a group, right-click the group, click **Exchange Tasks**, and follow the instructions in the Exchange Task Wizard. The Exchange Task Wizard helps you manage Exchange recipients by providing a set of tasks that apply to the selected group.

For more information, see [Exchange tasks on groups](#) later in this document.

Steps for performing Exchange tasks

To perform Exchange tasks on a group

1. In the console tree, locate and select the folder that contains the group.
2. In the details pane, right-click the group and click **Exchange Tasks**.
3. Follow the instructions in the Exchange Task Wizard.

NOTE:

- The Exchange Task Wizard helps you manage Exchange recipients by providing a set of tasks that applies to the groups. For more information, see [Steps for performing exchange tasks on groups](#).
- You can perform Exchange tasks on multiple groups at a time: Select the groups, right-click the selection, and click **Exchange Tasks** to start the Exchange Task Wizard.
- You can use the Find function of Active Roles in order to locate the groups on which you want to perform Exchange tasks. Once you have found the groups, you can start the Exchange Task Wizard as follows: Select the groups in the list of search results, right-click the selection, and click **Exchange Tasks**.

Moving groups

To move groups to another container, select the groups, right-click the selection, and click **Move**. In the **Move** dialog box, select the container to which you want to move the groups.

NOTE: The console provides the drag-and-drop function for moving objects. To move a group, you can drag it from the details pane to a destination container in the console tree.

Steps for moving a group

To move a group

1. In the console tree, locate and select the folder that contains the group.
2. In the details pane, right-click the group and click **Move** to display the **Move** dialog box.
3. In the **Move** dialog box, select the folder to which you want to move the group, and then click **OK**.

NOTE:

- With Active Roles, groups can only be moved within the same domain. This means that the group and the folder to which you want to move the group must belong to the same domain.
- You can move multiple groups at a time: Select the groups, right-click the selection, and click **Move** to display the **Move** dialog box. To select multiple groups, press and hold down CTRL, and then click each group.
- You can move objects, such as groups, by using the drag-and-drop feature. To move a selection of objects, drag the selection from the details pane to the destination container in the console tree.
- You can use the Find function of Active Roles in order to locate the group you want to move. Once you have found the group, you can move it as follows: Right-click the group in the list of search results and click **Move** to display the **Move** dialog box.

Exporting and importing groups

With the Active Roles console, you can export groups to an XML file and then import them from that file to populate a container in a different domain. The export and import operations provide a way to relocate groups between domains.

To export groups, select them, right-click the selection, and select **All Tasks | Export**. In the **Export Objects** dialog box, specify the file where you want to save the data, and click **Save**.

To import groups, right-click the container where you want to place the groups, and then click **Import**. In the **Import Directory Objects** dialog box, select the file to which the groups were exported, and click **Open**.

Deleting groups

To delete groups, select them, right-click the selection, and click **Delete**. Then, click **Yes** to confirm the deletion. If you select multiple groups, clicking **Delete** displays the **Delete Objects** dialog box. To delete all the selected groups, select the **Apply to all items** check box, and then click **Yes**.

NOTE: Deleting a group is an irreversible operation. A new group with the same name as a deleted group does not automatically assume the permissions and memberships of the deleted group. When recreating a deleted group, you need to manually add all permissions and memberships.

Steps for deleting a group

To delete a group

1. In the console tree, locate and select the folder that contains the group.
2. In the details pane, right-click the group, and then click **Delete**.

NOTE:

- Deleting a group is a permanent operation. Once a group has been deleted, all permissions and memberships associated with that group are permanently deleted. A new group with the same name as a previously deleted group does not automatically assume the permissions and memberships of the previously deleted group. To duplicate a deleted group, all permissions and memberships must be manually re-created.
- The confirmation message box displayed by the **Delete** command prompts you that you can *deprovision* rather than delete groups. The deprovision operation refers to a set of actions performed by Active Roles in order to prevent the use of there group. Active Roles comes with a default policy to automate some commonly-used deprovisioning tasks, and allows the deprovision policies to be adjusted as needed.
- You can deprovision a group as follows: Right-click the group in the details pane, and click **Deprovision**.
- You can use the Find function of Active Roles in order to locate the group you want to delete or deprovision. Once you have found the group, you can proceed as follows: Right-click the group in the list of search results, and click **Delete** or **Deprovision**.
- When deleting a group, you may encounter an error message stating that access is denied. A possible cause of this error is that the group is protected from deletion. To delete a protected group, you should first go to the **Object** tab in the **Properties** dialog box for that group, and clear the **Protect object from accidental deletion** check box.

Deprovisioning groups

Active Roles provides the ability to deprovision rather than delete groups. Deprovisioning a groups refers to a set of actions that are performed by Active Roles in order to prevent the use of the group.

The **Deprovision** command on a group updates the group object in Active Directory as prescribed by the deprovisioning policies. Active Roles comes with a default policy to automate some commonly-used deprovisioning tasks, and allows the administrator to configure and apply additional policies.

Steps for deprovisioning a group

To deprovision a group

1. In the console tree, locate and select the folder that contains the group you want to deprovision.

2. In the details pane, right-click the group, and then click **Deprovision**.
3. Wait while Active Roles updates the group.

NOTE:

- You can deprovision multiple groups at a time. Select two or more groups, right-click the selection, and then click **Deprovision**.
- The **Deprovision** command is also available in the Active Roles Web Interface.
- When you click the **Deprovision** command, the operation progress and results are displayed. When the operation is completed, Active Roles displays the operation summary, and allows you to examine operation results in detail.
- On a deprovisioned group, you can use the **Deprovisioning Results** command to view a report that lists the actions taken during the deprovisioning operation. For each action, the report informs about success or failure of the action. In the event of a failure, the report provides a description of the error situation.
- If a deprovisioned group needs to be restored (for example, if a group has been deprovisioned by mistake), the group can be reset to the state it was in before the deprovisioning occurred. This can be accomplished by using the **Undo Deprovisioning** command on the deprovisioned group.

Restoring deprovisioned groups

Active Roles provides the ability to restore deprovisioned groups. The purpose of this operation, referred to as the *Undo Deprovisioning* operation, is to roll back the changes that were made to a group by the Deprovision operation. When a deprovisioned group needs to be restored (for example, if a group has been deprovisioned by mistake), the Undo Deprovisioning operation allows the group to be restored to the state it was in before the changes were made.

Steps for restoring a deprovisioned group

To restore a deprovisioned group

1. In the console tree, locate and select the folder that contains the group you want to restore.
2. In the details pane, right-click the group, and then click **Undo Deprovisioning**.
3. Wait while Active Roles restores the group.
4. When you click the **Undo Deprovisioning** command, the operation progress and results are displayed. When the operation is completed, Active Roles displays the operation summary, and allows you to examine the operation results in detail. You can view a report that lists the actions taken during the restore operation. For each

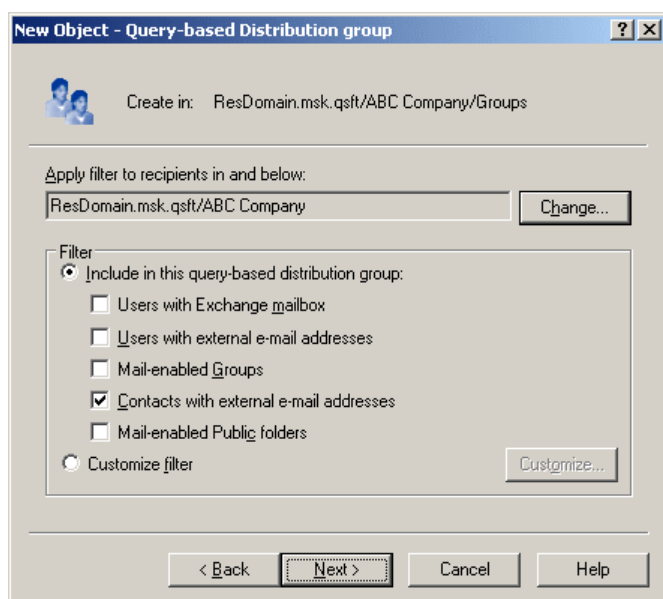
action, the report informs about success or failure of the action. In the event of a failure, the report provides a description of the error situation.

Administering query-based distribution groups

Query-based distribution group is a type of distribution group introduced in Exchange Server. The difference from the usual distribution group is that members of a query-based group are not statically placed into it. Email is propagated among the members of the group, but only among those of them who is currently in the state to comply with the specified LDAP query of this distribution group.

You can create a query-based distribution group as follows: in the console tree, right-click the container where you want to add the group, select **New | Query-based Distribution Group**, and then follow the instructions in the wizard. The following figure shows the step of the wizard where you can set up a query.

Figure 17: Administering query-based distribution groups



On this page, you can choose between predefined filters and custom filter. If select **Custom filter**, click **Customize** to configure the filter. This displays the **Custom Search** window where you can specify your search criteria.

You can manage a query-based distribution group in much the same way as you do with regular distribution groups: right-click the group and then select a command on the shortcut menu.

Steps for creating a query-based distribution group

To create a query-based distribution group

1. In the console tree, right-click the folder in which you want to add the group, and select **New | Query-based Distribution Group**.
2. In **Query-based Distribution Group name**, type a name for the group, and then click **Next**.
3. The box under **Apply filter to recipients in and below** displays the folder to search for recipients. Click **Change** to select the folder that contains the recipients you want the group to include.

The query returns only recipients in the selected folder and its sub-folders. To get the results that you want, you may have to select a parent folder or create multiple queries.

4. Under **Filter**, do one of the following:
 - Click **Include in this query-based distribution group**, and then click each item you want to include in the criteria for membership in the query-based distribution group. The following criteria are pre-defined:
 - **Users with Exchange mailbox**
 - **Users with external e-mail addresses**
 - **Groups that are mail-enabled**
 - **Contacts with external e-mail addresses**
 - **Public folders that are mail-enabled**
 - Click **Customize filter** and then click **Customize** to create your own criteria for the query.
5. Click **Next** to see a summary of the query-based distribution group you are about to create.
6. Click **Finish** to create the query-based distribution group. The new query-based distribution group is displayed in the details pane.
7. Right-click the query-based distribution group you just created and click **Properties**.
8. On the **Preview** tab, click **Start** to view the query results and verify that the correct recipients are included in the group.

NOTE:

- A query-based distribution group provides the same functionality as a standard distribution group, but instead of specifying static user memberships, a query-based distribution group allows you to use an LDAP query to dynamically build membership in the distribution group (for example "All full-time employees in my company").
- When creating a query-based distribution group, it is a good practice to use the Preview option. If the LDAP filter string contains bad formatting or incorrect LDAP syntax, the query-based distribution group does not work as expected: When a user sends mail to such a group, the user receives a non-delivery report (NDR). The **Preview** tab helps prevent you from constructing an incorrect query. Use the **Preview** tab to verify the validity and expected results of the query.
- The Preview option is useful not only for query validation, but also to determine how long it takes a query to run. Based on this time, you can decide whether to divide the query into smaller queries for better performance.

Administering dynamic (rule-based) groups

Active Roles provides the capability to automatically keep group membership lists up to date, eliminating the need to add and remove members manually. To automate the maintenance of group membership lists, Active Roles employs the following features:

- Rule-based mechanism that automatically adds and removes objects to groups whenever object attributes change in Active Directory.
- Flexible membership criteria that enable both query-based and static population of groups.

In Active Roles, rules-based groups are referred to as *dynamic groups*. The groups that have no membership rules specified are referred to as *basic groups*. Any security or distribution group can be converted to dynamic group by adding membership rules.

You can create a dynamic group by managing a basic group as follows: right-click the group, click **Convert to Dynamic Group**, select a rule type, and then configure a rule. For details, see "Steps for Adding a Membership Rule to a Group" in the Active Roles Administration Guide.

When you convert a basic group to a dynamic group, the group loses all members that were added to the group when it was basic. This is because the membership list of a dynamic group is entirely under the control of membership rules.

Once membership rules are added to a group, the group only includes the objects that comply with the membership rules. Active Roles overrides any changes made directly to the membership list by any administrative tool.

- NOTE:** In the Active Roles console, dynamic groups are marked with this icon: . Also, a special note on the **General** tab makes it possible to distinguish between dynamic groups and basic groups when using administrative tools other than Active Roles.

For dynamic groups, the **Properties** dialog box includes the **Membership Rules** tab. The **Members** tab for a dynamic group cannot be used to manage the membership list. It is only used to display a list of group members.

You can return a dynamic group to basic state as follows: right-click the group and click **Convert to Basic Group**. Then, click **Yes** to confirm the conversion. This operation removes all membership rules from the group. The group membership list remains intact as of the time of the conversion.

For more information about dynamic groups, refer to the “Dynamic Groups” chapter in the Active Roles Administration Guide or Active Roles Help.

Using temporal group memberships

By using temporal group memberships, you can manage group memberships of objects such as user or computer accounts that need to be members of particular groups for only a certain time period. This feature of Active Roles gives you flexibility in deciding and tracking what objects need group memberships and for how long.

This section guides you through the tasks of managing temporal group memberships in the Active Roles console. If you are authorized to view and modify group membership lists, then you can add, view and remove temporal group members as well as view and modify temporal membership settings on group members.

Adding temporal members

A temporal member of a group is an object, such as a user, computer or group, scheduled to be added or removed from the group. You can add and configure temporal members using the Active Roles console.

To add temporal members of a group

1. In the Active Roles console, right-click the group and click **Properties**.
2. On the **Members** tab in the **Properties** dialog box, click **Add**.
3. In the **Select Objects** dialog box, click **Temporal Membership Settings**.
4. In the **Temporal Membership Settings** dialog box, choose the appropriate options, and then click **OK**:
 - To have the temporal members added to the group on a certain date in the future, select **On this date** under **Add to the group**, and choose the date and time you want.
 - To have the temporal members added to the group at once, select **Now** under **Add to the group**.

- To have the temporal members removed from the group on a certain date, select **On this date** under **Remove from the group**, and choose the date and time you want.
 - To retain the temporal members in the group for indefinite time, select **Never** under **Remove from the group**.
5. In the **Select Objects** dialog box, type or select the names of the objects you want to make temporal members of the group, and click **OK**.
 6. Click **Apply** in the **Properties** dialog box for the group.

NOTE:

- To add temporal members of a group, you must be delegated the authority to add or remove members from the group. The appropriate authority can be delegated by applying the **Groups - Add/Remove Members** Access Template.
- You can make an object a temporal member of particular groups by managing properties of the object rather than properties of the groups. Open the **Properties** dialog box for that object, and then, on the **Member Of** tab, click **Add**. In the **Select Objects** dialog box, specify the temporal membership settings and supply the names of the groups as appropriate for your situation.

Viewing temporal members

The list of group members displayed by the Active Roles console makes it possible to distinguish between regular group members and temporal group members. It is also possible to hide or display so-called *pending members*, the temporal members that are scheduled to be added to the group in the future but are not actual members of the group so far.

To view temporal members of a group

1. In the Active Roles console, right-click the group and click **Properties**.
2. Examine the list on the **Members** tab in the **Properties** dialog box:
 - An icon of a small clock overlays the icon for the temporal members.
 - If the **Show pending members** check box is selected, the list also includes the temporal members that are not yet added to the group. The icons identifying such members are shown in orange.

The list of group memberships for a particular object makes it possible to distinguish between the groups in which the object is a regular member and the groups in which the object is a temporal member. It is also possible to hide or display so-called *pending group memberships*, the groups to which the object is scheduled to be added in the future.

To view groups in which an object is a temporal member

1. In the Active Roles console, right-click the object and click **Properties**.
2. Examine the list on the **Member Of** tab in the **Properties** dialog box:
 - An icon of a small clock overlays the icon for the groups in which the object is a temporal member.
 - If the **Show pending group memberships** check box is selected, the list also includes the groups to which the object is scheduled to be added in the future. The icons identifying such groups are shown in orange.

Rescheduling temporal group memberships

The temporal membership settings on a group member include the *start time* and *end time* settings.

The start time setting specifies when the object is to be actually added to the group. This can be specific date and time or an indication that the object should be added to the group right away.

The end time setting specifies when the object is to be removed from the group. This can be specific date and time or an indication that the object should not be removed from the group.

You can view or modify both the start time and end time settings using the Active Roles console.

To view or modify the start or end time setting for a member of a group

1. In the Active Roles console, right-click the group and click **Properties**.
2. In the list on the **Members** tab in the **Properties** dialog box, click the member and then click the **Temporal Membership Settings** button.
3. Use the **Temporal Membership Settings** dialog box to view or modify the start or end time settings.

The **Temporal Membership Settings** dialog box provides the following options:

- **Add to the group | Now** Indicates that the object should be added to the group at once.
- **Add to the group | On this date** Indicates the date and time when the object should be added to the group.
- **Remove from the group | Never** Indicates that the object should not be removed from the group.
- **Remove from the group | On this date** Indicates the date and time when the object should be removed from the group.

Regular members have the **Add to group** and **Remove from group** options set to **Already added** and **Never**, respectively. You can set a particular date for any of these options in order to convert a regular member to a temporal member.

NOTE:

- You can view or modify the start time and end time settings by managing an object rather than groups in which the object has memberships. Open the **Properties** dialog box for that object, and then, on the **Member Of** tab, select the group for which you want to manage the object's start or end time setting and click **Temporal Membership Settings**.
- On the **Members** or **Member Of** tab, you can change the start or end time setting for multiple members or groups at a time. From the list on the tab, select two or more items and click **Temporal Membership Settings**. Then, in the **Temporal Membership Settings** dialog box, select check boxes to indicate the settings to change and make the changes you want.

Removing temporal members

You can remove temporal group members in the same way as regular group members. Removing a temporal member of a group deletes the temporal membership settings for that object with respect to that group. As a result, the object will not be added to the group. If the object already belongs to the group at the time of removal, then it is removed from the group.

To remove a temporal member of a group

1. In the Active Roles console, right-click the group, and then click **Properties**.
2. On the **Members** tab in the **Properties** dialog box, click the member, click **Remove**, and then click **Apply**.

NOTE: You can remove an object that is a temporal member of a group by managing the object rather than the group. Open the **Properties** dialog box for that object, and then, on the **Member Of** tab, select the group from the list and click **Remove**.

Computer Account Management

- [About computer accounts](#)
- [Computer account management tasks](#)

About computer accounts

Computer accounts are Active Directory objects used to represent physical computers. Computer accounts allow computers to join the domain, and control their access to resources on the network. The operating system uses computer account information to determine access permissions for a computer.

Active Roles provides the facility to perform administrative tasks such as create, modify, and delete computer accounts. Active Roles can also be used to disable and enable accounts, add and remove accounts from groups, and reset accounts.

The following section describes how to use the Active Roles console to manage computer accounts. You can also use the Active Roles Web Interface to perform management tasks on computer accounts.

Computer account management tasks

This section covers the following tasks:

- [Creating a computer account](#)
- [Finding a computer account](#)
- [Modifying computer account properties](#)
- [Disabling and enabling a computer account](#)
- [Resetting a computer account](#)
- [Adding computer accounts to groups](#)
- [Removing a computer account from groups](#)

- [Moving computer accounts](#)
- [Exporting and importing computer accounts](#)
- [Deleting computer accounts](#)
- [Managing a remote computer](#)
- [Using Remote Desktop Connection](#)
- [Viewing BitLocker recovery passwords](#)

Creating a computer account

You can create a computer account as follows: in the console tree, right-click the container where you want to add the account, select **New | Computer**, and then follow the instructions in the wizard.

In the wizard, some property labels may be displayed as hyperlinks. In the following figure, these are **Computer name** and the **Computer name (pre-Windows 2000)**. The hyperlink indicates that Active Roles enforces certain policy restrictions on the property. To examine policy details, click the hyperlink: the policy information is displayed (see [Getting policy-related information](#) earlier in this document).

Figure 18: Creating a computer account

The policy information is also displayed whenever you supply a property value that violates a policy restriction. The wizard cannot proceed until you enter an acceptable value.

Steps for creating a computer account

To create a computer account

1. In the console tree, locate and select the folder in which you want to add the computer account.
2. Right-click the folder, point to **New** and click **Computer** to start the New Object - Computer wizard.
3. Follow the wizard pages to specify properties of the new computer account, such as the computer name and pre-Windows 2000 computer name.
4. If you want to set values for additional properties (those for which the wizard pages do not provide data entries), click **Edit Attributes** on the completion page of the wizard.
5. After setting any additional properties for the new computer account, click **Finish** on the completion page of the wizard.

NOTE:

- Normally, the rights of a domain administrator are required to join a computer to the domain through the use of an existing, newly created computer account. If you want to authorize a certain user or group to perform this task, you can do so when creating the computer account: Under **The following user or group can join this computer to a domain**, click **Change**, and then select the user or group you want.
- If the computer to be associated with the computer account you are creating is running a pre-Windows 2000 operating system, select the **Allow pre-Windows 2000 computers to use this account** check box.

Finding a computer account

To find a computer account, right-click the container you want to search and click **Find**. In the **Find** window, select **Computers** from the **Find** list, specify your search criteria, and start the search. In the search results list, you can right-click computer accounts and use commands on the shortcut menu to perform management tasks. For more information, see [Finding objects](#) earlier in this document.

Steps for finding a computer account

To find a computer account

1. On the **Action** menu, click **Find** to display the **Find** window.
2. In the **Find** box, click **Computers**.

3. In the **In** box, select the domain, container or Managed Unit you want to search, or click **Browse** to locate a domain, container or Managed Unit.
4. In the **Name** box, type the name of the computer account you want to find.
5. Optionally, in the **Role** list, click one of the following:
 - **Domain Controller** if you want to find only domain controllers
 - **Workstations and Servers** if you want to find only workstations and servers (not domain controllers)
6. Click **Find Now** to start your search.

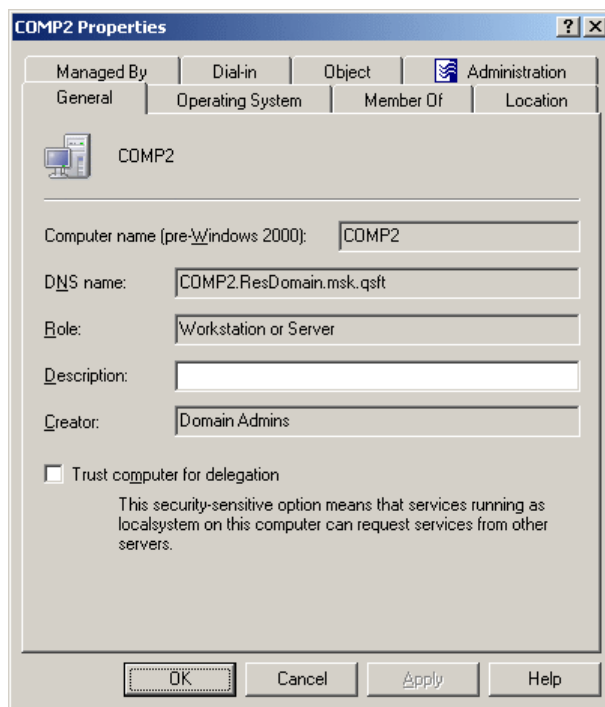
NOTE:

- You can manage found computer accounts directly from the list in the **Find** window: right-click a list item, and then use commands on the shortcut menu to perform management tasks.
- For more information on how to search for computers, see [Steps for searching for a computer](#) earlier in this document.
- You can use the **Advanced** tab for more powerful search options. For details, see [Steps for using advanced search options](#) earlier in this document.
- Replace this text with a description of a feature that is noteworthy.

Modifying computer account properties

To modify computer account properties, right-click the account, and then click **Properties**. You can make changes to computer account properties in the **Properties** dialog box, shown in the following figure.

Figure 19: Properties



In the **Properties** dialog box, some property labels may be displayed as hyperlinks. The hyperlink indicates that Active Roles enforces certain policy restrictions on the property. To examine policy details, click the hyperlink: the policy information is displayed (see [Getting policy-related information](#) earlier in this document).

The policy information is also displayed whenever you supply a property value that violates a policy restriction. Property changes cannot be applied until you enter an acceptable value.

You can use the **Properties** dialog box to view or modify any property of the computer account: go to the **Object** tab and click **Advanced Properties**. In the **Advanced Properties** window you can manage all properties, including those that cannot be accessed via the **Properties** dialog box itself.

You can also display the **Advanced Properties** window as follows: right-click the computer account and select **All Tasks | Advanced Properties**.

- NOTE:** In the console, you can select multiple computer accounts, right-click the selection, click **Properties**, and modify properties of all the selected accounts collectively via the **Properties** dialog box.

Steps for modifying computer account properties

To modify computer account properties

1. In the console tree, locate and select the folder that contains the computer account that you want to modify.
2. In the details pane, right-click the computer account you want to modify, and then click **Properties**.
3. Use the tabs in the **Properties** dialog box to view or modify properties of the computer account.
4. If you want to view or modify additional properties (those for which the tabs in the **Properties** dialog box do not provide data entries), go to the **Object** tab and click **Advanced Properties**.
5. After setting all the properties you want, click **OK**.

i NOTE:

- The behavior of the user interface elements in the **Properties** dialog box may vary depending on the configuration of Active Roles policies. To determine whether a given item on a tab is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the user interface elements.
- To modify properties for multiple computer accounts, press and hold down CTRL, and then click each account. Right-click the selection, and then click **Properties**.
- You can also access the **Advanced Properties** dialog box for a computer account as follows: Right-click the account and select **All Tasks | Advanced Properties**.
- You can use the Find function of Active Roles in order to locate the computer account that you want to modify. Once you have found the account, you can open the **Properties** dialog box for that account as follows: Right-click the account in the list of search results and click **Properties**.

Disabling and enabling a computer account

A computer account can be disabled as a security measure to prevent users from logging on to the computer, instead of deleting the computer account.

To disable a computer account, right-click the account and click **Disable Account**. To enable a computer account, right-click the account and click **Enable Account**. The **Enable Account** command only appears on disabled accounts. Disabled computer accounts are marked with the following icon: 

Steps for disabling a computer account

To disable a computer account

1. In the console tree, locate and select the folder that contains the computer account.
2. In the details pane, right-click the computer account and click **Disable Account**.

i NOTE:

- When you disable a computer account, the computer cannot authenticate to the domain until the account has been enabled.
- The **Disable Account** command is displayed if the account is enabled; otherwise, the **Enable Account** command is displayed on the menu. By using the **Enable Account** command you can change the status of the disabled account.

Steps for enabling a disabled computer account

To enable a disabled computer account

1. In the console tree, locate and select the folder that contains the computer account.
2. In the details pane, right-click the computer account and click **Enable Account**.

i NOTE: The **Enable Account** command is displayed if the account is disabled; otherwise, the **Disable Account** command is displayed on the menu.

Resetting a computer account

A computer account is normally reset if the computer has been taken offline and completely reinstalled. Resetting the account allows the (rebuilt) computer to rejoin the domain using the same name. If the computer account is reset whenever the computer has not been reinstalled, the computer cannot authenticate in the domain.

To reset a computer account, right-click the account, and click **Reset Account**. This command resets the computer account password. The **Reset Account** command is not available on domain controller accounts: resetting the password for domain controllers using this method is not allowed.

Adding computer accounts to groups

Adding a computer account to a group enables you to assign permissions to all computer accounts in the group, and to filter Group Policy settings on all accounts in the group.

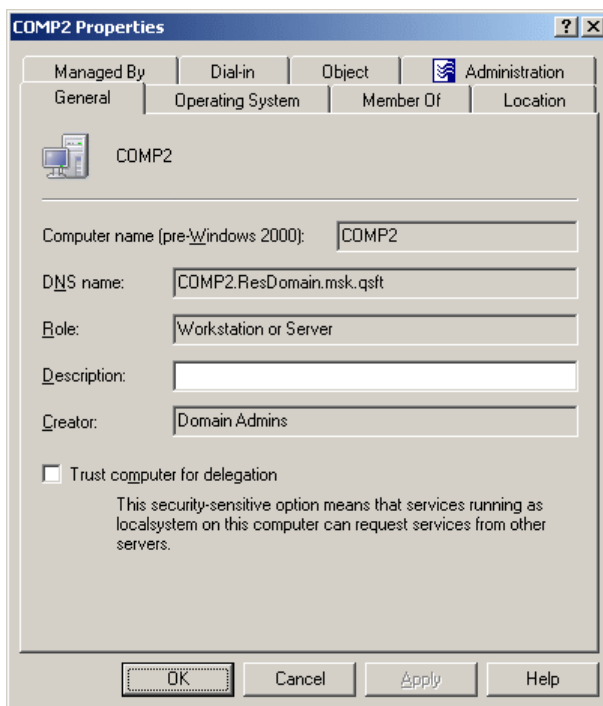
To add computer accounts to groups, select the accounts, right-click the selection, and click **Add to a Group**. This displays the **Select Objects** dialog box where you can select the groups to which you want to add the accounts (see [Adding user accounts to groups](#) earlier in this document).

You can also add a computer account to groups by modifying the group membership list on the **Member Of** tab in the **Properties** dialog box. To display the **Properties** dialog box, right-click the computer account and click **Properties**.

The **Member Of** tab lists the groups to which the computer account belongs, as shown in the following figure. If the **Show nested groups** check box is selected, the list also includes the groups to which the computer account belongs because of group nesting.

The **Temporal Membership Settings** button can be used to specify the date and time when the computer should be added or removed from the selected groups. For more information about this feature, see [Using temporal group memberships](#) earlier in this document.

Figure 20: Adding computer accounts to groups



On the **Member Of** tab, you can manage groups directly from the list of groups: right-click a group and use commands on the shortcut menu.

You can add the computer account to groups by clicking **Add** on the **Member Of** tab. This displays the **Select Objects** dialog box, allowing you to select the groups to which you want to add the computer account.

- NOTE:** When you select multiple computer accounts, the **Member Of** tab lists the groups to which all the selected accounts belong. If one of the accounts does not belong to a given group, that group does not appear in the list.

Steps for adding a computer account to a group

To add a computer account to a group

1. In the console tree, locate and select the folder that contains the computer account.
2. In the details pane, right-click the computer account, and then click **Add to a Group**.
3. Use the **Select Objects** dialog box to locate and select the group to which you want to add the computer account (you can select more than one group to add the account to).

i NOTE:

- You can add multiple computer accounts to a group at a time: Select the accounts, right-click the selection, and click **Add to a Group**. To select multiple accounts, press and hold down CTRL, and then click each account.
- You can also add or remove computer accounts from groups by using the **Properties** dialog box: Select one or more accounts, right-click the selection, click **Properties**, and go to the **Member Of** tab in the **Properties** dialog box.
- By adding a computer to a group, you can assign permissions to all of the computer accounts in that group and filter Group Policy settings on all accounts in that group.
- You can use the Find function of Active Roles in order to locate the computer accounts you want to add to a certain group. Once you have found the computer accounts, you can proceed as follows: Select the accounts in the list of search results, right-click the selection, and click **Add to a Group**.

Removing a computer account from groups

To remove a computer account from groups, right-click the account, click **Properties**, and go to the **Member Of** tab. On the **Member Of** tab, select groups from the list and click **Remove**.

Steps for removing a computer account from a group

To remove a computer account from a group

1. In the console tree, locate and select the folder that contains the computer account.
2. In the details pane, right-click the computer account, and then click **Properties**.

3. On the **Member Of** tab in the **Properties** dialog box, clear the **Show nested groups** check box, select the group from which you want to remove the computer account, and click **Remove**.

NOTE:

- If you have not cleared the **Show nested groups** check box, the list on the **Member Of** tab also includes the groups to which the computer account belongs indirectly, that is, because of group nesting. If you select such a group from the list, the **Remove** button is unavailable. A computer account can be removed from only those groups of which the account is a direct member.
- The computer account cannot be removed from its primary group (Domain Computers by default). You first need to change the computer's primary group: On the **Member Of** tab, select a different group from the list, and then click **Set Primary Group**.

Moving computer accounts

To move computer accounts to another container, select the accounts, right-click the selection, and then click **Move**. In the **Move** dialog box, select the container to which you want to move the accounts.

- NOTE:** The console provides the drag-and-drop function for moving objects. To move computer accounts, you can drag the selection from the details pane to a destination container in the console tree.

Steps for moving a computer account

To move a computer account

1. In the console tree, locate and select the folder that contains the computer account.
2. In the details pane, right-click the computer account and click **Move** to display the **Move** dialog box.
3. In the **Move** dialog box, select the folder to which you want to move the computer account, and then click **OK**.

NOTE:

- With Active Roles, computer accounts, as well as other directory objects, can only be moved within the same domain. This means that the folder to which you want to move the account must belong to the same domain as the account.
- You can move multiple computer accounts at a time: Select the accounts, right-click the selection, and click **Move** to display the **Move** dialog box. To select multiple accounts, press and hold down CTRL, and then click each account.
- You can use the Find function of Active Roles in order to locate the computer accounts you want to move. Once you have found the accounts, you can move them as follows: Select the accounts in the list of search results, right-click the selection, and click **Move** to display the **Move** dialog box.
- You can move objects, such as computer accounts, by using the drag-and-drop feature. To move a selection of objects, drag the selection from the details pane to the destination container in the console tree.

Exporting and importing computer accounts

With the Active Roles console, you can export computer accounts to an XML file and then import them from that file to populate a container in a different domain. The export and import operations provide a way to relocate computer accounts between domains.

To export computer accounts, select them, right-click the selection, and select **All Tasks | Export**. In the **Export Objects** dialog box, specify the file where you want to save the data, and click **Save**.

To import computer accounts, right-click the container where you want to place the accounts, and then click **Import**. In the **Import Directory Objects** dialog box, select the file to which the computer accounts were exported, and click **Open**.

Deleting computer accounts

To delete computer accounts, select them, right-click the selection, and click **Delete**. Then, click **Yes** to confirm the deletion. If you select multiple accounts, clicking **Delete** displays the **Delete Objects** dialog box. To delete all the selected accounts, select the **Apply to all items** check box, and then click **Yes**.

-  **NOTE:** Deleting a computer account is an irreversible operation. A new computer account with the same name as a deleted account cannot authenticate in the domain unless the administrator re-joins the computer to the domain. For this reason, it is recommended that you disable rather than delete computer accounts.

Steps for deleting a computer account

To delete a computer account

1. In the console tree, locate and select the folder that contains the computer account.
2. In the details pane, right-click the computer account, and then click **Delete**.

NOTE:

- You can delete multiple computer accounts at a time: Select the accounts, right-click the selection, and click **Delete**. To select multiple accounts, press and hold down CTRL, and then click each account.
- Once a computer account has been deleted, all permissions and memberships associated with that computer account are permanently deleted. Because the security ID (SID) for each account is unique, a new computer account with the same name as a previously deleted computer account does not automatically assume the permissions and memberships of the previously deleted account. To duplicate a deleted computer account, all permissions and memberships must be manually recreated.
- You can use the Find function of Active Roles in order to locate the computer accounts you want to delete. Once you have found the computer accounts, you can delete them as follows: Select the accounts in the list of search results, right-click the selection, and click **Delete**.
- When deleting a computer account, you may encounter an error message stating that access is denied. A possible cause of this error is that the computer account is protected from deletion. To delete a protected computer account, you should first go to the **Object** tab in the **Properties** dialog box for that computer account, and clear the **Protect object from accidental deletion** check box.

Managing a remote computer

The Active Roles console allows you to open the Computer Management console from which you can administer a remote computer. Computer Management combines several administration utilities into a single console, providing easy access to the computer's administrative properties and tools. You must have administrative rights on the computer to view certain information or to modify computer properties using Computer Management.

To manage a remote computer

1. In the console tree, locate and select the folder that contains the computer account of the computer you want to manage.
2. In the details pane, right-click the computer account, and then click **Manage** to open the Computer Management console.

NOTE: You can use the Find function of Active Roles to locate the computer account of the computer you want to manage. Once you have found the computer account, you can start Computer Management as follows: Right-click the computer account in the list of search results, and then click **Manage**.

Using Remote Desktop Connection

From the Active Roles console, you can access a computer through Remote Desktop Connection. The **Connect via RDP** command on a computer object allows you to establish a Remote Desktop Connection session to the computer represented by that computer object in Active Directory.

By supporting Remote Desktop Connection, Active Roles enables you to access a remote computer from your computer running the Active Roles console. However, the object representing the remote computer must be available in the console. This requires that the remote computer be a member of one of the domains managed by Active Roles. Additionally, the commonly-known requirements must be met that apply to Remote Desktop Connection: The remote computer must have Remote Desktop enabled, it must be available on the network, and it must be configured so that the user has permission to connect.

To access a computer through Remote Desktop Connection

1. In the Active Roles console, locate the desired computer object.
2. Right-click the computer object and then click **Connect via RDP**.

Viewing BitLocker recovery passwords

Active Roles allows you to locate and view BitLocker recovery passwords that are stored in Active Directory. This tool helps to recover data on a drive that has been encrypted by using BitLocker. You can examine a computer object's property pages to view the corresponding BitLocker recovery passwords. Additionally, you can perform a domain-wide search for a BitLocker recovery password.

Administrators can configure BitLocker Drive Encryption to back up recovery information for BitLocker-protected drives to Active Directory. Recovery information includes the recovery password for each BitLocker-protected drive, and the information required to identify which computers and drives the recovery information applies to. Backing up recovery passwords for BitLocker-protected drives allows administrators to recover the drive if it is locked, thereby ensuring that authorized persons can always access encrypted data belonging to the enterprise.

To view BitLocker recovery passwords, you must have been granted the appropriate permissions in Active Roles. The following Access Template provides sufficient permissions to view BitLocker recovery passwords:

- Computer Objects - View BitLocker Recovery Keys
- In addition, viewing BitLocker recovery passwords in a given Active Directory domain requires the following:
- The domain must be configured to store BitLocker recovery information (see “Backing Up BitLocker and TPM Recovery Information to AD DS” at <http://technet.microsoft.com/en-us/library/dd875529.aspx>).
- The computers protected by BitLocker must be joined to the domain.
- BitLocker Drive Encryption must have been enabled on the computers.

Steps for viewing BitLocker recovery passwords

The following procedures describe the most common tasks that apply to locating and viewing BitLocker recovery passwords.

To view the BitLocker recovery passwords for a computer

1. In the Active Roles console, locate the desired computer object.
2. Right-click the computer object, and then click **Properties**.
3. In the **Properties** dialog box, click the **BitLocker Recovery** tab to view the BitLocker recovery passwords that are associated with the computer you’ve selected.

To copy the BitLocker recovery password for a computer

1. Follow the steps in the previous procedure to view the BitLocker recovery passwords.
2. On the **BitLocker Recovery** tab of the **Properties** dialog box, perform the following steps:
 - a. In the **BitLocker Recovery Passwords** list, click the desired password ID.
 - b. Right-click in the **Details** box, click **Select All**, and then click **Copy**.
3. Press CTRL+V to paste the copied text to a destination location, such as a text file or spreadsheet.

You can use the Active Roles Web Interface to view the BitLocker recovery passwords for a computer: Select the computer object and then choose the **BitLocker Recovery** command.

To locate a BitLocker recovery password

1. In the Active Roles console or Web Interface, select the domain object, and then choose the **Find BitLocker Recovery Password** command.
2. On the **Find BitLocker Recovery Password** page, type the first eight characters of the BitLocker recovery key identification in the **Password ID (first 8 characters)** box, and then click **Search**.

You can also search for a BitLocker recovery password in all managed domains by choosing the **Find BitLocker Recovery Password** command on the **Active Directory** node in the Active Roles console or Web Interface.

Organizational Unit Management

- [About Organizational Units](#)
- [Organizational Unit management tasks](#)

About Organizational Units

Organizational Units (OUs) are containers in Active Directory. OUs can contain user accounts, groups, computer accounts, and other OUs. An object can be included in only one OU.

When you expand the **Active Directory** node in the Active Roles console, the console tree displays icons representing domains. You can double-click a domain icon to see containers that are defined in the domain. OUs are marked with the following icon: 

When you select an OU in the console tree, the details pane lists objects included in the OU, and the **Action** menu provides commands to create new objects in the OU, search for objects in the OU, and manage OU properties.

The following section guides you through the Active Roles console to manage Organizational Units. You can also use the Active Roles Web Interface to perform management tasks on Organizational Units.

Organizational Unit management tasks

This section covers the following tasks:

- [Creating an Organizational Unit](#)
- [Finding an Organizational Unit](#)
- [Modifying Organizational Unit properties](#)
- [Renaming an Organizational Unit](#)

- [Moving an Organizational Unit](#)
- [Deleting an Organizational Unit](#)

Creating an Organizational Unit

You can create an OU as follows: in the console tree, right-click the domain or another OU, select **New | Organizational Unit**, and then follow the instructions in the wizard.

On the first page of the wizard, type the name for the new OU in the **Name** box. If necessary, select or clear the **Protect container from accidental deletion** check box. Click **Next** and then click **Finish** to complete the operation.

By selecting the **Protect container from accidental deletion** check box you ensure that the newly created OU cannot be deleted, whether using Active Roles or other tools for Active Directory administration. When somebody attempts to delete an OU for which this check box is selected, the operation returns an error indicating that access is denied. For an existing OU, you can view or change this setting on the **Object** tab in the **Properties** dialog box.

Steps for creating an Organizational Unit

To create an Organizational Unit

1. In the console tree, locate and select the folder in which you want to add the Organizational Unit.
2. Right-click the folder, point to **New** and click **Organizational Unit** to start the New Object - Organizational Unit wizard.
3. Follow the wizard pages to specify properties of the new Organizational Unit, such as the name of the Organizational Unit.
4. If you want to set values for additional properties (those for which the wizard pages do not provide data entries), click **Edit Attributes** on the completion page of the wizard.
5. After setting any additional properties for the new Organizational Unit, click **Finish** on the completion page of the wizard.

NOTE: To create an Organizational Unit, you can also click the domain node or folder in which you want to add the Organizational Unit, and then click  on the toolbar.

Finding an Organizational Unit

To find an Organizational Unit, select the domain you want to search, and click **Find**. In the **Find** window, select **Organizational Units** from the **Find** list, specify your search criteria,

and start the search. In the search results list, you can right-click Organizational Units and use commands on the shortcut menu to perform management tasks. For more information, see [Finding objects](#) earlier in this document.

Steps for finding an Organizational Unit

To find an Organizational Unit

1. On the **Action** menu, click **Find** to display the **Find** window.
2. In the **Find** box, click **Organizational Units**.
3. In the **Name** box, type the name of the Organizational Unit you want you want to find.
4. Click **Find Now** to start your search.

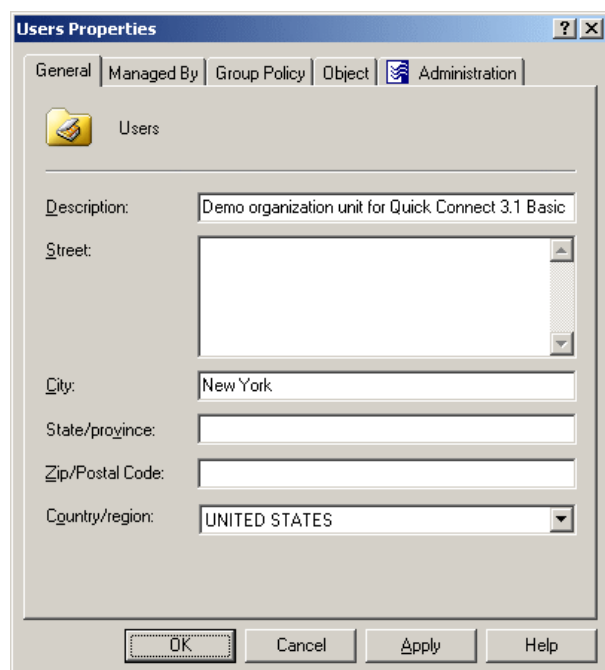
i NOTE:

- You can manage found Organizational Units directly from the list in the **Find** window: right-click a list item, and then use commands on the shortcut menu to perform management tasks.
- For more information on how to search for Organizational Units, see [Steps for searching for an Organizational Unit](#) earlier in this document.
- You can use the **Advanced** tab for more powerful search options. For details, see [Steps for using advanced search options](#) earlier in this document.

Modifying Organizational Unit properties

To modify properties of an OU, right-click the OU, and then click **Properties**. You can make changes to OU properties in the **Properties** dialog box, shown in the following figure.

Figure 21: Modifying Organizational Unit properties



In the **Properties** dialog box, some property labels may be displayed as hyperlinks. The hyperlink indicates that Active Roles enforces certain policy restrictions on the property. To examine policy details, click the hyperlink: the policy information is displayed (see [Getting policy-related information](#) earlier in this document).

The policy information is also displayed whenever you supply a property value that violates a policy restriction. Property changes cannot be applied until you enter an acceptable value.

You can use the **Properties** dialog box to view or modify any property of the Organizational Unit: go to the **Object** tab and click **Advanced Properties**. In the **Advanced Properties** window you can manage all properties, including those that cannot be accessed via the **Properties** dialog box itself.

You can also display the **Advanced Properties** window as follows: right-click the Organizational Unit and select **All Tasks | Advanced Properties**.

Steps for modifying Organizational Unit properties

To modify Organizational Unit properties

1. In the console tree, locate the Organizational Unit you want to modify.
2. Right-click the Organizational Unit, and then click **Properties** to display the **Properties** dialog box for that Organizational Unit.

3. Use the tabs in the **Properties** dialog box to view or modify properties of the Organizational Unit.
4. If you want to view or modify additional properties (those for which the tabs in the **Properties** dialog box do not provide data entries), go to the **Object** tab and click **Advanced Properties**.
5. After setting all the properties you want, click **OK**.

NOTE:

- You can also access the **Advanced Properties** dialog box for an Organizational Unit as follows: Right-click the Organizational Unit and select **All Tasks | Advanced Properties**.
- You can use the Find function of Active Roles in order to locate the Organizational Unit that you want to modify. Once you have found the Organizational Unit, you can open the **Properties** dialog box as follows: Right-click the Organizational Unit in the list of search results and click **Properties**.

Renaming an Organizational Unit

To rename an OU, right-click the OU, and click **Rename**. Type the new name and press ENTER.

Steps for renaming an Organizational Unit

To rename an Organizational Unit

1. In the console tree, locate the Organizational Unit you want to rename.
2. Right-click the Organizational Unit, and then click **Rename**.
3. Type a new name, and then press ENTER.

NOTE: You can use the Find function of Active Roles in order to locate the Organizational Unit that you want to rename. Once you have found the Organizational Unit, you can rename it as follows: Right-click the Organizational Unit in the list of search results and click **Rename**.

Moving an Organizational Unit

To move an OU, right-click the OU, and click **Move**. In the **Move** dialog box, select the container to which you want to move the OU.

NOTE: The console provides the drag-and-drop function for moving objects. To move an OU, you can drag it to a destination container in the console tree.

Steps for moving an Organizational Unit

To move an Organizational Unit

1. In the console tree, locate the Organizational Unit you want to move.
2. Right-click the Organizational Unit, and then click **Move** to display the **Move** dialog box.
3. In the **Move** dialog box, select the folder to which you want to move the Organizational Unit, and then click **OK**.

i NOTE:

- With Active Roles, Organizational Units, as well as other directory objects, can only be moved within the same domain. This means that the destination folder must belong to the same domain as the Organizational Unit you want to move.
- You can move an Organizational Unit by using the drag-and-drop feature: To move an Organizational Unit, drag it from the details pane to the destination container in the console tree.

Deleting an Organizational Unit

To delete an OU, right-click the OU, and click **Delete**. If the OU contains any objects, the **Delete Objects** dialog box appears. You can delete the OU and all objects it contains: select the **Apply to all items** check box, and click **Yes**.

Steps for deleting an Organizational Unit

To delete an Organizational Unit

1. In the console tree, locate the Organizational Unit you want to delete.
2. Right-click the Organizational Unit, and click **Delete**.

i NOTE:

- If the selected Organizational Unit contains other objects, the console prompts you to confirm the deletion of the objects within the Organizational Unit. You can cancel the deletion of the Organizational Unit if you do not want to delete the objects it contains. Another option is to delete the Organizational Unit along with all the objects it contains.
- When deleting an Organizational Unit, you may encounter an error message stating that access is denied. A possible cause of this error is that the Organizational Unit is protected from deletion. To delete a protected Organizational Unit, you should first go to the **Object** tab in the **Properties** dialog box for that Organizational Unit, and clear the **Protect object from accidental deletion** check box.

Management of Contacts

- [About contacts](#)
- [Contact management tasks](#)

About contacts

A contact is an Active Directory object that holds e-mail and telephone information about an individual, without giving that person a security account on the network.

Contacts do not have a security identifier, unlike user accounts and groups. Contacts are used to add members to distribution lists or groups without granting them access to network resources.

You can use Active Roles to create, modify, and delete contacts. You can also perform Exchange-related tasks such as establishing email addresses for contacts.

The following section describes how to use the Active Roles console to manage contacts. You can also use the Active Roles Web Interface to perform contact management tasks.

Contact management tasks

This section covers the following tasks:

- [Creating a contact](#)
- [Finding a contact](#)
- [Modifying contact properties](#)
- [Renaming a contact](#)
- [Adding and removing contacts from groups](#)
- [Performing Exchange tasks on a contact](#)
- [Moving contacts](#)

- [Exporting and importing contacts](#)
- [Deleting contacts](#)

Creating a contact

You can create a new contact as follows: in the console tree, right-click the container where you want to add the contact, select **New | Contact**, and then follow the instructions in the wizard.

In the wizard, some property labels may be displayed as hyperlinks. In the following figure, this is **Full name**. The hyperlink indicates that Active Roles enforces certain policy restrictions on this property. To examine policy details, click the hyperlink: the policy information is displayed (see [Getting policy-related information](#) earlier in this document).

Figure 22: Creating a contact

The policy information is also displayed whenever you supply a property value that violates a policy restriction. The wizard cannot proceed until you enter an acceptable value.

Steps for creating a contact

To create a contact

1. In the console tree, locate and select the folder in which you want to add the contact.
2. Right-click the folder, point to **New** and click **Contact** to start the New Object - Contact wizard.

3. Follow the wizard pages to specify properties of the new contact, such as the contact's first name, last name, full name, display name, and Exchange e-mail address settings.
4. If you want to set values for additional properties (those for which the wizard pages do not provide data entries), click **Edit Attributes** on the completion page of the wizard.
5. After setting any additional properties for the new contact, click **Finish** on the completion page of the wizard.

Finding a contact

To find a contact, right-click the container you want to search and click **Find**. In the **Find** window, select **Contacts** from the **Find** list, specify your search criteria, and start the search. In the search results list, you can right-click contacts and use commands on the shortcut menu to perform management activities.

For step-by-step instructions on how to search for contacts, see [Steps for searching for a user, contact, or group](#) earlier in this document.

Modifying contact properties

To modify contact properties, right-click the contact, and then click **Properties**. You can make changes to contact properties in the **Properties** dialog box, shown in the following figure.

Figure 23: Modifying contact properties

The screenshot shows the 'Robert Finn Properties' dialog box. It has a main title bar with a question mark and close button. Below the title bar are three tabs: 'Exchange Advanced', 'Object', and 'Administration'. Under the 'Object' tab, there are four sub-tabs: 'General', 'Address', 'Telephones', and 'Organization'. The 'General' sub-tab is selected. In the 'General' sub-tab, there are three main sections: 'Alias' with a text field containing 'RobertFinn', 'E-mail' with a text field containing 'SMTP:BFinn@company.com' and a 'Modify...' button, and 'Receiving message size' with two radio buttons: 'Use default limit' (selected) and 'Maximum (KB):' with an empty text field. Below these is a 'Message restrictions' section with a label 'Accept messages:' and four radio buttons: 'From authenticated users only', 'From everyone' (selected), 'Only from:', and 'From everyone except:'. Below the 'Only from:' and 'From everyone except:' radio buttons is an empty text field and two buttons: 'Add...' and 'Remove...'. At the bottom of the dialog are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

In the **Properties** dialog box, some property labels may be displayed as hyperlinks. The hyperlink indicates that Active Roles enforces certain policy restrictions on the property. To examine policy details, click the hyperlink: the policy information is displayed (see [Getting policy-related information](#) earlier in this document).

The policy information is also displayed whenever you supply a property value that violates a policy restriction. Property changes cannot be applied until you enter an acceptable value.

You can use the **Properties** dialog box to view or modify any property of the contact: go to the **Object** tab and click **Advanced Properties**. In the **Advanced Properties** window you can manage all properties, including those that cannot be accessed via the **Properties** dialog box itself.

You can also display the **Advanced Properties** window as follows: right-click the contact and select **All Tasks | Advanced Properties**.

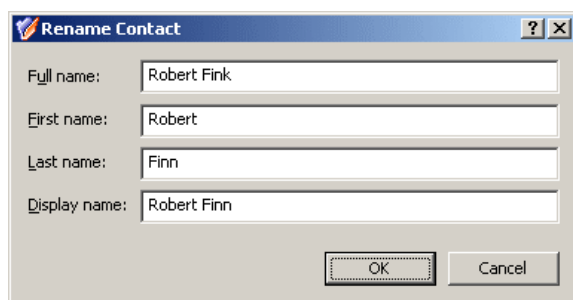
- NOTE:** In the console, you can select multiple contacts, right-click the selection, click **Properties**, and then modify properties of all the selected contacts collectively via the **Properties** dialog box.

The instructions on how to manage contact properties are similar to those for user accounts, see [Steps for modifying user account properties](#) earlier in this document.

Renaming a contact

To rename a contact, right-click the contact and click **Rename**. Type a new name and press ENTER. This displays the **Rename Contact** dialog box where you can change the first name, last name, and display name of the contact.

Figure 24: Rename Contact



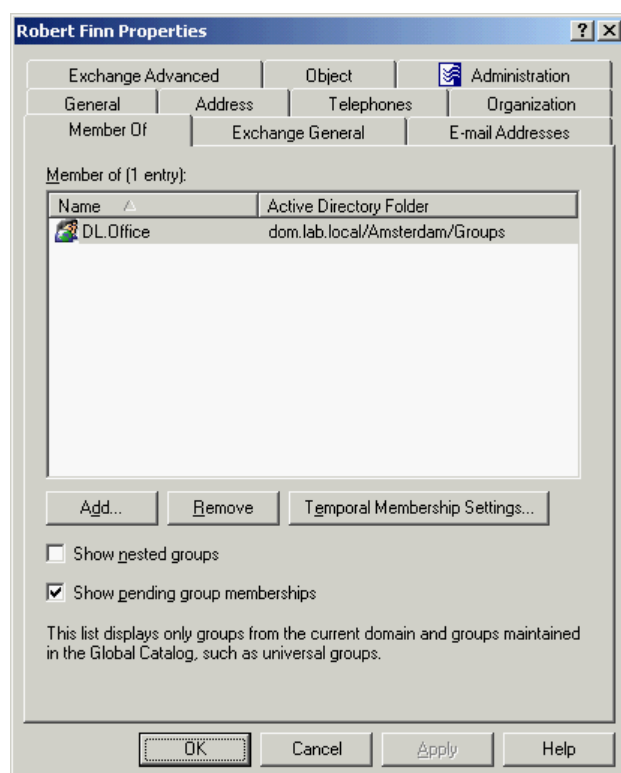
The screenshot shows a 'Rename Contact' dialog box. It has a title bar with a question mark icon and a close button. The dialog contains four text input fields: 'Full name:' with the value 'Robert Finn', 'First name:' with 'Robert', 'Last name:' with 'Finn', and 'Display name:' with 'Robert Finn'. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

Adding and removing contacts from groups

To add contacts to groups, select the contacts, right-click the selection, and click **Add to a Group**. This displays the **Select Objects** dialog box where you can select the groups to which you want to add the contacts (see [Adding user accounts to groups](#) earlier in this document).

You can also add or remove a contact from groups by modifying the group membership list on the **Member Of** tab in the **Properties** dialog box. To display the **Properties** dialog box, right-click the contact and click **Properties**. The **Member Of** tab looks as shown in the following figure.

Figure 25: Adding and removing contacts from groups



The **Member Of** tab lists the groups to which the contact belongs. If the **Show nested groups** check box is selected, the list also includes the groups to which the contact belongs due to group nesting.

The **Temporal Membership Settings** button can be used to specify the date and time when the contact should be added or removed from the selected groups. For more information about this feature, see [Using temporal group memberships](#) earlier in this document.

You can modify the list on the **Member Of** tab using the **Add** and **Remove** buttons. Clicking **Add** displays the **Select Objects** dialog box where you can type or select the names of the groups you want to add to the list. Clicking **Remove** deletes the selection from the list.

Performing Exchange tasks on a contact

To perform Exchange tasks on a contact, right-click the contact, click **Exchange Tasks**, and follow the instructions in the Exchange Task Wizard. The Exchange Task Wizard helps you manage Exchange recipients by providing a set of tasks that apply to the selected contact.

For more information, see [Exchange tasks on contacts](#) later in this document.

Steps for performing Exchange tasks

To perform Exchange tasks on a contact

1. In the console tree, locate and select the folder that contains the contact.
2. In the details pane, right-click the contact and click **Exchange Tasks**.
3. Follow the instructions in the Exchange Task Wizard.

i NOTE:

- The Exchange Task Wizard helps you manage Exchange recipients by providing a set of tasks that applies to the contacts. For more information, see [Steps for performing Exchange tasks on contacts](#).
- You can perform Exchange tasks on multiple contacts at a time: Select the contacts, right-click the selection, and click **Exchange Tasks** to start the Exchange Task Wizard.
- You can use the Find function of Active Roles in order to locate the contacts on which you want to perform Exchange tasks. Once you have found the contacts, you can start the Exchange Task Wizard as follows: Select the contacts in the list of search results, right-click the selection, and click **Exchange Tasks**.

Moving contacts

To move contacts to another container, select the contacts, right-click the selection, and then click **Move**. In the **Move** dialog box, select the container to which you want to move the contacts.

- i** NOTE: The console provides the drag-and-drop function for moving objects. To move contacts, you can drag the selection from the details pane to a destination container in the console tree.

Exporting and importing contacts

With the Active Roles console, you can export contacts to an XML file and then import them from that file to populate a container in a different domain. The export and import operations provide a way to relocate contacts between domains.

To export contacts, select them, right-click the selection, and select **All Tasks | Export**. In the **Export Objects** dialog box, specify the file where you want to save the data, and click **Save**.

To import contacts, right-click the container where you want to place the contacts, and then click **Import**. In the **Import Directory Objects** dialog box, select the file to which the contacts were exported, and click **Open**.

Deleting contacts

To delete contacts, select them, right-click the selection, and click **Delete**. Then, click **Yes** to confirm the deletion. If you select multiple contacts, clicking **Delete** displays the **Delete Objects** dialog box. To delete all the selected contacts, select the **Apply to all items** check box, and then click **Yes**.

NOTE:

- Deleting a contact is an irreversible operation. A new contact with the same name as a deleted contact does not automatically assume the same membership of distribution and security groups that the deleted contact had.
- When deleting a contact, you may encounter an error message stating that access is denied. A possible cause of this error is that the contact is protected from deletion. To delete a protected contact, you should first go to the **Object** tab in the **Properties** dialog box for that contact, and clear the **Protect object from accidental deletion** check box.

Management of Exchange Recipients

- [Creating an Exchange mailbox](#)
- [Performing Exchange tasks](#)
- [Managing Exchange-related properties](#)
- [Managing Unified Messaging users](#)

Creating an Exchange mailbox

When creating a user account, the Active Roles console provides the option to create a user mailbox for that user. User mailboxes are the most commonly used mailbox type, and it is typically the mailbox type that is assigned to users in an Exchange organization.

Additionally, the console provides a number of commands for creating special-purpose mailboxes in an Exchange organization where Exchange 2013 or later is deployed. On a container, such as an organizational unit, each of these commands creates a disabled user account along with a special-purpose mailbox associated with that account:

- **New | Room Mailbox** Creates a mailbox that is assigned to a meeting location, such as a conference room, auditorium, or training room. Room mailboxes can be included as resources in meeting requests, providing a simple and efficient way of organizing meetings for your users.
- **New | Equipment Mailbox** Creates a mailbox that is assigned to a non-location specific resource, such as a portable computer projector, microphone, or a company car. Equipment mailboxes can be included as resources in meeting requests, providing a simple and efficient way of utilizing resources for your users.
- **New | Linked Mailbox** Creates a mailbox that is assigned to an individual user in a separate, trusted forest. Linked mailboxes may be necessary for organizations that choose to deploy Exchange in a resource forest. The resource forest scenario allows an organization to centralize Exchange in a single forest, while allowing access to the Exchange organization with user accounts in one or more trusted forests.
- **New | Shared Mailbox** Creates a mailbox that is not primarily assigned to a single user and is generally configured to allow logon access for multiple users. The user account that is associated with a shared mailbox must be a disabled account. It is

possible to specify a list of the mailbox users each of which will have full access to the shared mailbox.

Steps for creating a user mailbox

This section provides instructions on how to create a user mailbox upon creation of a new user account. To create a user mailbox for an existing user account, use the **Exchange Tasks** command on that account. For details, see [Steps for performing Exchange tasks on a user account](#).

NOTE: Mailboxes can be created only for **Users**, enabling mailbox for a **Contact** is not allowed.

To create a new user mailbox

1. In the console tree, locate and select the folder in which you want to add the user account.
2. Right-click the folder, point to **New** and then click **User**.
3. Follow the wizard pages to specify properties of the new user account, such as the user first name, last name, full name, display name, logon name, pre-Windows 2000 logon name, and password.
4. When prompted for the user alias and mailbox location, accept or change the default alias setting, and select the mailbox database to hold the mailbox data. Optionally, specify a retention policy, Exchange ActiveSync mailbox policy, or address book policy for this mailbox.
5. Click **Finish** on the completion page of the wizard.

NOTE: The behavior of the wizard pages may vary depending on the configuration of Active Roles policies. To determine whether a given item on a page is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the wizard pages.

Steps for creating a room or equipment Mailbox

This section provides instructions on how to create a room or equipment mailbox along with a new disabled user account that will be associated with the mailbox. To create a room or equipment mailbox associated with an existing disabled user account, use the **Exchange Tasks** command on that account. For details, see [Steps for performing Exchange tasks on a user account](#).

To create a new room or equipment mailbox

1. In the console tree, locate and select the folder in which you want to add the user account.
2. Right-click the folder, point to **New** and then click one of the following:
 - Click **Room Mailbox** to create a room mailbox.
 - Click **Equipment Mailbox** to create an equipment mailbox.
3. Follow the wizard pages to specify properties of the new user account, such as the user first name, last name, full name, display name, logon name, pre-Windows 2000 logon name, and password.
4. When prompted for the user alias and mailbox location, accept or change the default alias setting, and select the mailbox database to hold the mailbox data. Optionally, specify a retention policy, Exchange ActiveSync mailbox policy, or address book policy for this mailbox.
5. When prompted for the resource mailbox settings, specify the resource capacity and select the resource custom properties to add to the mailbox.

These settings are optional. After the mailbox has been created, you can view or change these settings on the **Resource Information** tab in the **Properties** dialog box for the user account associated with the mailbox.

6. Click **Finish** on the completion page of the wizard.

Steps for creating a linked mailbox

This section provides instructions on how to create a linked mailbox along with a new disabled user account that will be associated with the mailbox. To create a linked mailbox associated with an existing disabled user account, use the **Exchange Tasks** command on that account. For details, see [Steps for performing Exchange tasks on a user account](#).

To create a new linked mailbox

1. In the console tree, locate and select the folder in which you want to add the user account.
2. Right-click the folder, point to **New** and then click **Linked Mailbox**.
3. Follow the wizard pages to specify properties of the new user account, such as the user first name, last name, full name, display name, logon name, pre-Windows 2000 logon name, and password.
4. When prompted for the user alias and mailbox location, accept or change the default alias setting, and select the mailbox database to hold the mailbox data. Optionally, specify a retention policy, Exchange ActiveSync mailbox policy, or address book policy for this mailbox.
5. When prompted for the linked master account, click **Browse** and select the user from a trusted forest or domain to which you want to assign the mailbox.

After the mailbox has been created, you can view or change this setting on the **Master Account** tab in the **Properties** dialog box for the user account associated with the mailbox.

6. Click **Finish** on the completion page of the wizard.

Steps for creating a shared mailbox

This section provides instructions on how to create a shared mailbox along with a new disabled user account that will be associated with the mailbox. To create a shared mailbox associated with an existing disabled user account, use the **Exchange Tasks** command on that account. For details, see [Steps for performing Exchange tasks on a user account](#).

To create a new shared mailbox

1. In the console tree, locate and select the folder in which you want to add the user account.
2. Right-click the folder, point to **New** and then click **Shared Mailbox**.
3. Follow the wizard pages to specify properties of the new user account, such as the user first name, last name, full name, display name, logon name, pre-Windows 2000 logon name, and password.
4. When prompted for the user alias and mailbox location, accept or change the default alias setting, and select the mailbox database to hold the mailbox data. Optionally, specify a retention policy, Exchange ActiveSync mailbox policy, or address book policy for this mailbox.
5. When prompted to specify the users who will have full access to the shared mailbox, click the **Add** button and then select the users you want.

This setting is optional. After the mailbox has been created, you can add or remove mailbox users on the **Mailbox Sharing** tab in the **Properties** dialog box for the user account associated with the mailbox.

6. Click **Finish** on the completion page of the wizard.

Performing Exchange tasks

The Active Roles console provides the Exchange Task Wizard to perform the following tasks on existing users, groups, and contacts:

- Create and disable user mailboxes.
- Enable a user for Unified Messaging (UM), disable UM for a user, reset a user's UM PIN.
- Create and disable special-purpose mailboxes.
- Enable and disable archiving for user mailboxes.

- Establish external e-mail addresses for users, contacts, and groups.
- Delete external e-mail addresses for users, contacts, and groups.
- Move mailboxes to a different mailbox store or mailbox database.
- Remove all Exchange settings (advanced, disaster-recovery task).

The following sections briefly describe the Exchange tasks available on user accounts, groups, and contacts.

Exchange tasks on user accounts

To perform Exchange tasks on user accounts, select one or more accounts, right-click the selection, click **Exchange Tasks**, and then follow the instructions in the wizard. Depending on the selected accounts, the following tasks are available.

If the user account is mailbox-enabled (the user account has an Exchange mailbox associated with it):

- **Disable Mailbox** Disconnects the mailbox and marks the mailbox for deletion.
- **Move Mailbox** Moves the mailboxes to a different server. In case of Exchange 2013 or later, creates and starts a mailbox move request.
- **Enable Unified Messaging** Enables the user account for Unified Messaging. For details, see [Managing Unified Messaging users](#) later in this document.
- **Enable Archive** Creates an archive mailbox for the user mailbox (requires Exchange 2013 or later).
- **Disable Archive** Disconnects the archive mailbox from the user mailbox (requires Exchange 2013 or later).

If the user account is mail-enabled (the user account has an associated e-mail address but does not have an associated Exchange mailbox):

- **Delete E-Mail Addresses** Deletes the e-mail addresses from the user account.

If the user account is neither mailbox-enabled nor mail-enabled:

- **Create User Mailbox** Creates a user mailbox for the selected user.
- **Create Room Mailbox** Creates a mailbox for room scheduling. The user account associated with this mailbox type must be a disabled account.
- **Create Equipment Mailbox** Creates a mailbox for equipment scheduling. The user account associated with this mailbox type must be a disabled account.
- **Create Linked Mailbox** Creates a mailbox that is assigned to a certain user in a separate, trusted forest. The user account associated with this mailbox type must be a disabled account.
- **Create Shared Mailbox** Creates a mailbox that allows logon access for multiple users. The user account associated with this mailbox type must be a disabled account.

- **Establish E-Mail Addresses** Establishes an external e-mail address for the selected user.

Steps for performing Exchange tasks on a user account

To perform Exchange tasks on a user account

1. Right-click the user account and click **Exchange Tasks** to start the Exchange Task wizard.
2. On the **Available Tasks** page of the wizard, select the task you want to perform.

The following tasks are available, depending upon the selected account:

- The account is enabled, and does not have a mailbox or external e-mail address - **Create User Mailbox, Establish E-mail Addresses**
 - The account is disabled, and does not have a mailbox or external e-mail address - **Create User Mailbox, Create Room Mailbox, Create Equipment Mailbox, Create Linked Mailbox, Create Shared Mailbox, Establish E-mail Addresses**
 - The account has a mailbox - **Move Mailbox, Disable Mailbox**
 - The account has an external e-mail address - **Delete E-mail Addresses**
 - The account has a user mailbox without an archive - **Enable Archive**
 - The account has a user mailbox with an archive - **Disable Archive**
3. On the next page of the wizard, do one of the following, depending on the selected task:
 - **Mailbox Settings** Specify the alias and mailbox database. You can select a retention policy, Exchange ActiveSync mailbox policy, or address book policy for the mailbox.
 - **Enable Archive** Optionally, specify the mailbox database for the archive.
 - **Resource Information** Configure the resource capacity and custom properties for the room or equipment mailbox.
 - **Master Account** Select the master account for the linked mailbox.
 - **Mailbox Sharing** Specify the users who you want to have access to the mailbox.
 - **Establish E-mail Addresses** Specify the user alias and external e-mail address.
 - **Move Mailbox** Select the database to which you want to move the mailbox. If the mailbox has an archive enabled, specify whether to move only the mailbox, only the archive, or both the mailbox and the archive.
 - **Disable Mailbox, Disable Archive, Delete E-mail Addresses,** Confirm the operation.

4. On the completion page of the wizard, review the results of the task. To view the progress report, click **Back**. To close the wizard, click **Finish**.

Move Mailbox task in Exchange 2013 or later

When performing the **Move Mailbox** task, Active Roles leverages the move request functionality provided by Exchange 2013 or later. A mailbox move operation is asynchronous in the sense that Active Roles only creates a move request, letting Exchange Server perform the request in the background. For details on the move request functionality, see Microsoft's article "Understanding Move Requests" at <http://technet.microsoft.com/en-us/library/dd298174.aspx>.

The **Move Mailbox** task creates a mailbox move request, which causes Exchange Server to start the process of moving the mailbox. The move request is performed in an asynchronous fashion by the Exchange Mailbox Replication service. While the service is performing the move request, and after the move request is completed, you can view the status of the move request by using the Active Roles console or Web Interface.

To view the status of a move request by using the Active Roles console

1. Open the **Properties** dialog box for the user account whose mailbox move is requested.
2. In the **Properties** dialog box, click the **Exchange Advanced** tab, and then click **Mailbox Move Status**.
3. In the **Mailbox Move Status** dialog box, under **Move request status**, view the status of the move request.

To view the status of a move request by using the Active Roles Web Interface

1. Open the **Exchange Properties** page for the user account whose mailbox move is requested.
2. On the **Exchange Properties** page, click the **Advanced** tab, and then click **Mailbox Move Status**.
3. In the **Mailbox Move Status** dialog box, under **Move request status**, view the status of the move request.

The **Move request status** field displays one of the following statuses:

- **Move not requested** The move of the mailbox was not requested.
- **Automatically suspended** The move of the mailbox is ready to complete, but it was suspended because the move request was created with the option to suspend the mailbox move when it is ready to complete.
- **Completed** The move of the mailbox was completed successfully without any warnings.
- **Completed with warning** The move of the mailbox was completed, but there were certain warnings during the mailbox move process.

- **Completion in progress** The mailbox is in its final stages of being moved. If this is an online mailbox move, at this point, the mailbox may become unavailable to the user.
- **Failed** The move of the mailbox has failed.
- **In progress** The move of the mailbox is in progress. If this is an online mailbox move, the user can access the mailbox. If this is an offline mailbox move, the mailbox is unavailable.
- **Queued** The mailbox move request has been queued, and is waiting to be picked up by the Exchange Mailbox Replication service.
- **Suspended** The move of the mailbox was suspended by using the Suspend-MoveRequest cmdlet of the Exchange Management Shell.
- When a move request reaches a status of **Completed** or **Completed with warning**, the request is not considered finished. Rather, the request is preserved so that you can examine the move operation results. You will not be able to move the mailbox again until you finish the previous move request. You can finish the request by clicking **Clear Move Request** in the **Mailbox Move Status** dialog box.

When you clear a completed move request, information about that request is deleted from Exchange Server, and the InTransit flag is removed from the mailbox so a new request to move the mailbox can be created if needed. The **Clear Move Request** command is only available if the request has a status of **Completed** or **Completed with warning**.

If a mailbox move request is not yet completed, you can cancel the request by clicking **Remove Move Request** in the **Mailbox Move Status** dialog box. When you remove a move request that is in progress, mailbox replication stops, and the replica of the mailbox is deleted from the destination mailbox database. If you later decide to move the mailbox, you will have to perform the **Move Mailbox** task at the beginning.

Exchange tasks on groups

To perform Exchange tasks on groups, select one or more groups, right-click the selection, click **Exchange Tasks**, and then follow the instructions in the wizard. The following tasks are available for groups:

- **Establish an E-Mail Address** Establishes an e-mail address for each selected group to configure it as a distribution list.
- **Delete E-Mail Addresses** Deletes the e-mail address from each selected group so that the group can no longer be used as a distribution list.

Steps for performing exchange tasks on groups

To perform Exchange tasks on a group

1. Right-click the group, and then click **Exchange Tasks** to start the Exchange Task Wizard.
2. On the **Available Tasks** page of the wizard, select the task you want to perform.
The following tasks are available, depending upon the selected group:
 - The group has no e-mail address established - **Establish E-mail Address**
 - The group has an e-mail address established - **Delete E-mail Addresses**
3. On the next page of the wizard, do one of the following, depending on the selected task:
 - **Establish E-mail Addresses** Modify the alias of the group, if needed. By default, the alias is the same as the name of the group.
 - **Delete E-mail Addresses** Confirm the deletion of the e-mail addresses.
4. On the completion page of the wizard, review the results of the task. To view the progress report, click **Back**. To close the wizard, click **Finish**.

Exchange tasks on contacts

To perform Exchange tasks on contacts, select one or more contacts, right-click the selection, click **Exchange Tasks**, and then follow the instructions in the wizard. The following tasks are available for contacts:

- **Establish E-Mail Addresses** Establishes an external e-mail address for each selected contact.
- **Delete E-Mail Addresses** Deletes the e-mail addresses from each selected contact.

Steps for performing Exchange tasks on contacts

To perform Exchange tasks on a contact

1. Right-click the contact, and then click **Exchange Tasks** to start the Exchange Task Wizard.
2. On the **Available Tasks** page of the wizard, select the task you want to perform.
The following tasks are available, depending upon the selected contact:
 - The contact has no e-mail address established - **Establish E-mail Addresses** (establishes an external e-mail address for the selected contact to include the

- address in the Exchange address list)
- Contact has an e-mail address established - **Delete E-mail Addresses**
3. On the next page of the wizard, do one of the following, depending on the selected task:
 - **Establish E-mail Addresses** Specify the contact's alias and external e-mail address.
 - **Delete E-mail Addresses** Confirm the operation.
 4. On the completion page of the wizard, review the results of the task. To view the progress report, click **Back**. To close the wizard, click **Finish**.

Managing Exchange-related properties

For Exchange recipients (mail-enabled users, contacts and groups, and mailbox-enabled users) the **Properties** dialog box includes the following tabs for managing Exchange-related properties:

- [Exchange General tab](#)
- [Exchange Advanced tab](#)
- [E-mail Addresses tab](#)
- [Mail Flow Settings tab](#)
- [Mailbox Settings tab](#)
- [Mailbox Features tab](#)
- [Calendar Settings tab](#)
- [Resource Information tab](#)
- [Master Account tab](#)
- [Mailbox Sharing tab](#)

Exchange General tab

For a mailbox-enabled user account, you can use the **Exchange General** tab to:

- Identify the mailbox type
- Identify the organizational unit of the mailbox user account
- Identify who last logged on to the mailbox
- Identify the number of items held in the mailbox, and the size of the mailbox
- Identify the mailbox database and server
- Identify the archive database is an archive is enabled for the mailbox

- View the date and time that the configuration of the mailbox was last modified
- View or change the alias
- Hide the mailbox from Exchange address lists
- View or change custom attributes
- For a mail-enabled user account or contact, you can use the **Exchange General** tab to:
 - View or change the alias
 - View or change the option to use MAPI rich text format
 - Hide the user or contact from Exchange address lists
 - View or change custom attributes

For a mail-enabled (distribution) group, you can use the **Exchange General** tab to:

- View or change the alias and display name
- View or change custom attributes

Exchange Advanced tab

For a mailbox-enabled user account, you can use the **Exchange Advanced** tab to:

- View or change the simple display name

The simple display name is used by systems that cannot interpret all of the characters in a normal display name.

- Downgrade high priority mail bound for X.400

Use this option to downgrade e-mail that is set for high priority delivery to an X.400-type e-mail address. The downgrade causes the outbound e-mail to conform to original 1984 X.400 conventions.

- View or change the Internet Locator Service (ILS) settings

You can specify the Internet Locator Service (ILS) server and ILS account name for the mailbox.

- View or change mailbox rights

You can specify mailbox permissions, assign mailbox permissions to users and groups, and change inherited permissions.

- View mailbox move status

You can view status of mailbox move request, clear completed move request, or remove non-completed move request.

For a mail-enabled user or contact, you can use the **Exchange Advanced** tab to:

- View or change the simple display name
- Downgrade high priority mail bound for X.400 (for a mail-enabled user)
- View or change the Internet Locator Service (ILS) settings

For a mail-enabled (distribution) group, you can use the **Exchange Advanced** tab to:

- View or change the simple display name
- Select the desired expansion server

You can select a server in your Exchange organization that will be responsible for expanding the membership list for this mail-enabled (distribution) group.

- Hide the group from Exchange address lists
- Choose whether to send out-of-office messages to message originators
- Select delivery report options

E-mail Addresses tab

For a mailbox-enabled user account or a mail-enabled (distribution) group, you can use the **E-mail Addresses** tab to:

- View, add, edit or remove e-mail addresses
- View or change the default reply address for each address type
- Set the option to update e-mail addresses based on e-mail address policy

For a mail-enabled user account or contact, you can use the **E-mail Addresses** tab to:

- View, add, edit or remove e-mail addresses
- View or change the default reply address for each address type
- View or change the external e-mail address
- Set the option to update e-mail addresses based on e-mail address policy

Mail Flow Settings tab

For a mailbox-enabled user account, you can use the **Mail Flow Settings** tab to:

- View or change delivery options

You can allow one or more users to send messages on behalf of the mailbox user, specify a forwarding address for messages addressed to the mailbox, and limit the number of recipients to whom the mailbox user can send a message.

- View or change message size restrictions and message delivery restrictions

You can specify the maximum size of incoming and outgoing messages for the mailbox, and from whom the mailbox can or cannot receive e-mail.

For a mail-enable user account or contact, you can use the **Mail Flow Settings** tab to:

- View or change message size restrictions and message delivery restrictions
You can specify the maximum size of incoming messages for the user or contact, and from whom the user or contact can or cannot receive e-mail.

For a mail-enabled (distribution) group, you can use the **Mail Flow Settings** tab to:

- View or change message size restrictions and message delivery restrictions
You can specify the maximum size of incoming messages for the distribution group, and from whom the group can or cannot receive e-mail.
- View or change the message moderation settings
You can configure whether messages sent to the distribution group must be approved by a moderator before they are delivered to the distribution group members.

Mailbox Settings tab

For a user account that has a mailbox on Exchange 2013 or later, you can use the **Mailbox Settings** tab to:

- View or change the messaging records management settings
You can select or suspend retention policy for the mailbox, place the mailbox on litigation hold to preserve deleted mailbox items and to record change made to mailbox items, specify the messaging records management description URL, and provide mailbox comments.
- View or change storage quotas
You can specify storage limits that, when exceeded, result in the mailbox user being warned or prohibited from sending or receiving e-mail. You can also select the number of days a deleted item is retained in the mailbox store before it is permanently deleted.
- View or change the archive quota
If archiving is enabled for the mailbox, you can view or change the archive size at which messages are no longer moved to the archive and a warning message is sent to the mailbox user.
- Apply a sharing policy to the mailbox
You can select the sharing policy you want to be associated with the mailbox. This enables the mailbox user to create sharing relationships with users in other external federated Exchange organizations or with individuals in non-Exchange organizations.
- Apply a role assignment policy to the mailbox
You can select the management role assignment policy you want to be associated with the mailbox. This policy controls what specific mailbox and distribution group configuration settings the mailbox user is allowed to modify.

- Apply an address book policy to the mailbox

You can select the address book policy you want to be associated with the mailbox. This policy defines the global address list and other address lists that the user will see in Outlook and Outlook Web App.

Mailbox Features tab

You can use the **Exchange Features** tab to manage a variety of mailbox features for the mailbox user. You can also change configuration settings for certain features by selecting a feature from the list, and then clicking **Properties**.

The **Mailbox Features** tab includes the following settings:

- **Outlook Mobile Access** Allows the user to browse the mailbox with a cell phone or other wireless devices.
- **Exchange ActiveSync** Allows the user to access the mailbox from a mobile device.
Select this setting, and then click **Properties** to apply an Exchange ActiveSync mailbox policy to the mailbox.
- **Up-to-date Notifications** Allows the user to apply notifications in order to keep the mailbox data on a mobile device always up to date.
- **IMAP4** Allows the user to access the mailbox from an IMAP4 client such as Outlook Express.
Select this setting, and then click **Properties** to configure the MIME format of messages that are retrieved from the server for the mailbox. You can use the protocol default or specify a custom setting that takes precedence over the default protocol settings.
- **POP3** Allows the user to access the mailbox from a POP3 client such as Outlook Express.
Select this setting, and then click **Properties** to configure the MIME format of messages that are retrieved from the server for the mailbox. You can use the protocol default or specify a custom setting that takes precedence over the default protocol settings.
- **Outlook Web App** Allows the user to access the mailbox from a Web browser by using Microsoft Outlook Web App (formerly Outlook Web Access).
Select this setting, and then click **Properties** to assign an Outlook Web App mailbox policy to the mailbox. In Exchange 2013 or later, Outlook Web App mailbox policies can be used to manage access to Outlook Web App features, overriding the settings of the Outlook Web App virtual directory. Earlier versions of Exchange do not provide for Outlook Web App mailbox policies.
- **MAPI** Allows the user to access the mailbox from a MAPI client such as Microsoft Outlook.

- **Archive** If the mailbox is archive-enabled, you can view or change the archive properties.

To enable or disable archiving for the mailbox, use the **Enable Archive** or **Disable Archive** task in the Exchange Task wizard. If an archive is enabled for the mailbox, click **Properties** to view or change the name of the archive associated with this mailbox.

- **Unified Messaging** If the mailbox is enabled for Unified Messaging, you can view or change the Unified Messaging properties of the mailbox.

To enable or disable the mailbox for Unified Messaging, use the **Enable Unified Messaging** or **Disable Unified Messaging** task in the Exchange Task wizard. If the mailbox is enabled for Unified Messaging, click **Properties** to view or change the Unified Messaging properties of this mailbox. For more information and instructions, see [Managing Unified Messaging users](#) later in this document.

Calendar Settings tab

You can use the **Calendar Settings** tab to view or change the Calendar Attendant settings for the mailbox. The tab is available on (disabled) user accounts associated with a room or equipment mailbox in Exchange 2013.

The Calendar Attendant processes meeting requests as they come in, even if users are not currently logged on by means of a client such as Outlook. When enabled, the Calendar Attendant updates the time of the meeting on an attendee's calendar after receiving an update from the meeting organizer, and updates the attendee's response on the meeting organizer's calendar after receiving a response from the attendee.

The **Calendar Settings** tab provides the option to enable or disable the Calendar Attendant for the mailbox, and provides a number of options to control how the Calendar Attendant handles meeting requests and responses. If you enable the Calendar Attendant, the following options are available:

- **Remove meeting forward notifications to the Deleted Items folder** This option causes the Calendar Attendant to delete notifications about forwarded meeting requests. Such a notification occurs when a meeting request created by the mailbox user is forwarded to a new recipient by one of the meeting attendees.
- **Remove old meeting requests and responses** This option causes the Calendar Attendant to delete out-of-date meeting requests and responses from the mailbox's Inbox folder.
- **Mark new meeting requests as Tentative** This option causes the Calendar Attendant to automatically place new meeting requests on the mailbox user's calendar and mark them as tentative, without sending a reply to the meeting organizer.
- **Process meeting requests and responses originating outside the Exchange organization** This option causes the Calendar Attendant to automatically process requests and responses from people that don't have a mailbox in the Exchange organization.

Resource Information tab

On the **Resource Information** tab, you can view or change the resource mailbox settings. This tab is available only for resource mailboxes. For instructions on how to create a resource mailbox, see [Steps for creating a room or equipment Mailbox](#) earlier in this document.

There are two types of resource mailboxes in Microsoft Exchange Server: room and equipment. *Room mailboxes* are assigned to a meeting location such as a conference room, auditorium, or training room. *Equipment mailboxes* are assigned to a resource that is not location specific, such as a portable computer projector, microphone, or company car.

The following fields provide users with general information about the resource:

- **Resource capacity** Use this box on the **Resource Information** tab to type the capacity the resource can handle. For example, for a room mailbox, you can specify the number of people the room can accommodate. The value range is from 0 through 2,147,483,647.
- **Resource custom properties** Custom resource properties can help users select the most appropriate room or equipment by providing additional information about the resource. For example, suppose a custom property for room mailboxes called **Audio-Visual** is defined in your Exchange organization. You can add this property to the room mailboxes for the rooms that have audio-visual equipment. This allows users to identify which conference rooms have audio-visual equipment available.

Click the **Add** button on the **Resource Information** tab to open a dialog box allowing you to select custom properties. The dialog box displays a list of all custom resource properties that are defined in your Exchange organization for the specific resource type (room or equipment). Select the custom resource properties you want to assign to this mailbox, and then click **OK**.

Use the **Remove** button to remove custom resource property from the resource mailbox.

With Exchange 2013 or later, the following additional options are available:

- **Enable the Resource Booking Attendant** Select this check box to allow the Resource Booking Attendant to process resource booking requests and cancellations. When enabled, the Resource Booking Attendant uses the booking policies to determine whether incoming requests will be accepted or declined. If the Resource Booking Attendant is not enabled, the resource mailbox's delegate must accept or decline all requests.
- **Resource policy** Click this button to view or change the options that determine under which conditions the resource mailbox automatically accepts requests. For further information, see [Resource Policy](#) later in this topic.
- **Resource information** Click this button to view or change the options that specify the information that appears in the resource's calendar. For details, see [Resource Information](#) later in this topic.

- **Resource in-policy requests** Click this button to specify the users who are allowed to submit requests within the resource's policy configuration. For details, see [Resource In-Policy Requests](#) later in this topic.
- **Resource out-of-policy requests** Click this button to specify the users who are allowed to submit requests that don't meet the resource's policy configuration. For details, see [Resource Out-of-Policy Requests](#) later in this topic.

Resource Policy

Use the **Resource Policy** dialog box to specify under which conditions the resource mailbox automatically accepts requests:

- **Allow conflict meeting requests** Select this check box to allow conflicting meeting requests to be scheduled by the Resource Booking Attendant.
- **Allow repeating meetings** Select this check box to allow repeating or recurring meetings to be scheduled.
- **Allow scheduling only during working hours** Select this check box to allow scheduling for the resource to occur during working hours. Users can set working hours by using Outlook or Outlook Web App.
- **Reject repeating meetings that have an end date beyond the booking window** Select this check box to allow the Resource Booking Attendant to reject recurring meeting requests that are outside of the resources booking window.
- **Booking window (days)** Use this box to specify the number of days that the resource can be booked in advance. For example, if the booking window is set for 90 days and a request is received for scheduling the resource 4 months from today's date, the Resource Booking Attendant rejects the request.
- **Maximum duration (minutes)** Use this box to specify the maximum number of minutes that the resource can be scheduled for.
- **Maximum conflict instances** Use this box to specify the maximum number of conflicts allowed for recurring meetings. If the number of instances for a recurring meeting in conflict exceeds this number, the recurring meeting request is declined.
- **Conflict percentage allowed** Use this box to specify the conflict percentage threshold from recurring meetings. If the percentage of instances of a recurring meeting that conflicts with other meetings exceeds the threshold, the recurring meeting request is declined.
- **Specify delegates of this mailbox** Click **Add** to add delegates who can control the scheduling options for the resource mailbox. Click **Remove** to remove delegates from this resource mailbox.
- **Forward meeting requests to delegates** Select this check box to forward all meeting requests to the delegates.

Resource Information

Use the **Resource Information** dialog box to specify the meeting information that appears in the resource's calendar:

- **Delete attachments** Select this check box to remove attachments from all incoming requests.
- **Delete comments** Select this check box to remove any text in the message body of incoming requests.
- **Delete the subject** Select this check box to remove the subject of all incoming requests.
- **Delete non-calendar items** Select this check box to remove all non-calendar Outlook items received by the mailbox.
- **Add the organizer's name to the subject** Select this check box to specify whether the resource requester's name is added to the subject of the request.
- **Remove the private flag on an accepted meeting** Select this check box to clear the private flag for all incoming requests.
- **Send organizer information when a meeting request is declined because of conflicts** Select this check box to send the meeting organizer information regarding declined requests.
- **Customize the response message that organizers will receive** Select the **Add additional text** check box to customize the message that the requester receives when the meeting has been declined, and then type the additional information in the **Additional text** field.
- **Mark pending requests as Tentative on the calendar** Select this check box to specify that all pending requests are marked as Tentative in the resource's calendar. The delegate can then accept or deny the request as needed.

Resource In-Policy Requests

Use the **Resource In-Policy Requests** dialog box to specify the users who are allowed to submit requests within the resource policy's configuration:

- **Specify users who are allowed to submit in-policy meeting requests that will be automatically approved** Click **All users** or **Selected recipients**. If you click **Selected recipients**, you need to click **Add** to select the recipients. You can also remove selected recipients by clicking **Remove**.
- **Specify who can submit in-policy meeting requests that are subject to approval by a resource mailbox delegate** Click **All users** or **Selected recipients**. If you click **Selected recipients**, you need to click **Add** to select the recipients. You can also remove selected recipients by clicking **Remove**.

Resource Out-of-Policy Requests

Use the **Resource Out-of-Policy Requests** dialog box to specify the users who are allowed to submit resource requests that don't meet the resource's policy configuration. Users who have permission to submit out-of-policy requests won't have their request denied, but the requests require approval by one of the resource's delegates:

- **All users** Choose this option to allow all users to submit out-of-policy requests.
- **Selected recipients** Choose this option to allow specific users to submit out-of-policy requests. If you choose this option, you need to click **Add** to select the users. You can also remove selected users by clicking **Remove**.

Master Account tab

Use the **Master Account** tab to view or change information about the master account for the linked mailbox. This tab is available only for linked mailboxes. For instructions on how to create a linked mailbox, see [Steps for creating a linked mailbox](#) earlier in this document.

Linked mailboxes are mailboxes that are accessed by users in a separate, trusted forest. Linked mailboxes may be necessary for organizations that choose to deploy Exchange in a resource forest. The resource forest scenario allows an organization to centralize Exchange in a single forest, while allowing access to the Exchange organization with user accounts in one or more trusted forests. The linked master account is the user account that will be used to access the linked mailbox.

From the **Master Account** tab you can view the current master account or choose a different master account for the linked mailbox. Click the **Browse** button next to the **Linked master account** box and then use the **Select Objects** dialog box to select the user account you want to be used to access this linked mailbox. Select a user account from a forest or domain trusted by the forest or domain where Exchange is deployed.

Mailbox Sharing tab

Use the **Mailbox Sharing** tab to view or change information about the users who have full access to the shared mailbox. This tab is available only for shared mailboxes. For instructions on how to create a shared mailbox, see [Steps for creating a shared mailbox](#) earlier in this document.

Shared mailboxes are generally configured to allow logon access for multiple users. Although it is possible to grant additional users the logon rights to any mailbox type, shared mailboxes are dedicated for this functionality. The user account that is associated with a shared mailbox must be a disabled account. From this page, you can grant permissions to all users that require access to the shared mailbox.

From this tab, you can view or change a list of mailbox users. These are the users who can log on to the shared mailbox and have full access to the mailbox contents. They can use the

mailbox to send and receive messages, manage contacts, schedule meetings, and maintain a task list. You can add or remove mailbox users:

- Click the **Add** button on the **Mailbox Sharing** tab and then use the **Select Objects** dialog box to select the users you want to have full access to the shared mailbox.
- If you want a certain user to no longer have access to the shared mailbox, select that user from the **Mailbox users** list and click the **Remove** button.

Managing Unified Messaging users

You can use Active Roles to configure Unified Messaging users. Unified Messaging is a technology in Microsoft Exchange Server that combines voice messaging and e-mail messaging into one store, accessible from a telephone and a computer. Unified Messaging puts all e-mail and voice messages into one Exchange mailbox that can be accessed from many different devices. Once a user has an Exchange mailbox, you can configure the user for Unified Messaging. This can be accomplished by using the Active Roles console or Web Interface.

This section provides information on how to perform the following tasks of managing Unified Messaging users:

- [Enable a user for Unified Messaging](#)
- [View or change the properties of a UM-enabled user](#)
- [Reset Unified Messaging PIN for a UM-enabled user](#)
- [Disable Unified Messaging for a user](#)

Enable a user for Unified Messaging

When you enable a user for Unified Messaging (UM), a default set of UM properties are applied to the user, and the user will be able to use the Unified Messaging features. You have the option to add a Session Initiation Protocol (SIP) or E.164 address for the user. However, the user must still have an extension number configured.

You can configure the extension number automatically or manually when enabling the user for Unified Messaging. An extension number is required for each UM-enabled user associated with a telephone extension, SIP Uniform Resource Identifier (URI), or E.164 dial plan. The extension number must be the correct number of digits, as specified in the UM dial plan for the UM mailbox policy. If the user is associated with an E.164 dial plan, you can manually configure an E.164 address for the user when you are enabling the user for Unified Messaging. If you associate a user to a SIP URI or E.164 dial plan, you must manually enter an extension number and the SIP or E.164 address for the user.

To enable a user for Unified Messaging

1. Do one of the following, depending on whether you are using the Active Roles console or Web Interface:
 - a. In the Active Roles console,
 - b. Right-click the user, and then click **Exchange Tasks**;
 - c. Follow the steps in the Exchange Task wizard;
 - d. On the **Available Tasks** page, click **Enable Unified Messaging**, and then click **Next**.
 - e. In the Web Interface, click the user, and then click the **Enable Unified Messaging** command.
2. On the **Unified Messaging Mailbox Policy** page, complete the following field:
 - a. **Unified Messaging mailbox policy** Click **Browse** and select the Unified Messaging mailbox policy that you want to associate with the user's mailbox.

Unified Messaging (UM) mailbox policies define settings such as PIN policies and dialing restrictions. Each UM-enabled user must be associated with a certain UM mailbox policy.

3. Click **Next**.
4. On the **Unified Messaging PIN** page, complete the following fields:
 - **Automatically generate PIN to access Outlook Voice Access** Select this option to automatically generate a Unified Messaging PIN for the user. This is the default setting. If you select this option, a PIN is automatically generated based on the PIN policies configured on the user's UM mailbox policy. The automatically generated PIN will be sent in an e-mail message to the user's mailbox.
 - **Manually specify PIN** Select this option to manually specify a Unified Messaging PIN for the user. The PIN you specify with this option will be sent in an e-mail message to the user's mailbox.
 - **Manually specify PIN** Select this option to manually specify a Unified Messaging PIN for the user. The PIN you specify with this option will be sent in an e-mail message to the user's mailbox.

The PIN must comply with the PIN policies configured on the user's UM mailbox policy. For example, if the UM mailbox policy is configured to accept only PINs that contain five or more digits, you must specify a PIN at least five digits long.

 - **Require user to reset PIN at first telephone logon** Select this check box to force the user to reset the Unified Messaging PIN the first time that the user accesses the Unified Messaging system from a telephone. It is a security best practice to force UM-enabled users to change their PIN upon their first logon to help protect against unauthorized access to their mailbox data.

5. Click **Next**.

6. On the **Extension Configuration** page, complete the following fields:

- **Automatically-generated mailbox extension** Select this option if you want the extension number for the user's mailbox to be automatically generated from the telephone number specified in Active Directory. This option is selected by default if the user's UM mailbox policy is associated with a Telephone Extension dial plan; otherwise, the option is unavailable. The automatically generated extension will be sent in an e-mail message to the user's mailbox.
- The automatically generated extension will comply with the number of digits specified on the dial plan for the user's UM mailbox policy. For example, if the dial plan is configured to use 5-digit extension numbers, the Unified Messaging server will take the last 5 digits of the user's telephone number and use those digits as the user's mailbox extension.
- **Manually-entered mailbox extension** Select this option if you want to manually specify the extension number for the user's mailbox. The extension number you specify with this option will be sent in an e-mail message to the user's mailbox.
- The extension must comply with the number of digits specified on the dial plan for the user's UM mailbox policy. For example, if the dial plan is configured to use 5-digit extension numbers, you should specify an extension containing exactly 5 digits.
- **Automatically-generated SIP resource identifier** Select this option if you want the SIP resource identifier or SIP address for the user's mailbox to be automatically generated. If Microsoft Office Communications Server is deployed in your organization, then the user's SIP address is taken from the msRTCSIP-PrimaryUserAddress attribute in Active Directory. If this attribute is not populated, the user's primary SMTP address will be used for the SIP address, such as john.smith@company.com.
- **Automatically-generated SIP resource identifier** Select this option if you want the SIP resource identifier or SIP address for the user's mailbox to be automatically generated. If Microsoft Office Communications Server is deployed in your organization, then the user's SIP address is taken from the msRTCSIP-PrimaryUserAddress attribute in Active Directory. If this attribute is not populated, the user's primary SMTP address will be used for the SIP address, such as john.smith@company.com.
- This option is available only if the user's UM mailbox policy is associated with a SIP URI dial plan. This option will be unavailable if the user's UM mailbox policy is associated with a Telephone Extension or E.164 dial plan.
- This option is available only if the user's UM mailbox policy is associated with a SIP URI dial plan. This option will be unavailable if the user's UM mailbox policy is associated with a Telephone Extension or E.164 dial plan.
- This option also requires that you manually enter a mailbox extension for the user. This extension number is used when the user accesses the mailbox via Outlook Voice Access. The number of digits in the extension number must

match the number of digits configured on the SIP URI dial plan for the user's UM mailbox policy.

- **Manually-entered SIP resource identifier** Select this option if you want to manually enter the SIP or E.164 address for the user. This option is available if the user's UM mailbox policy is associated with either a SIP URI or E.164 dial plan. This option will be unavailable if the user's UM mailbox policy is associated with a Telephone Extension dial plan.
- If the user's UM mailbox policy is associated with an E.164 dial plan, you have to enter an E.164 address for the user. The address must be in the correct E.164 format, such as +14275551234. If the user's UM mailbox policy is associated with a SIP URI dial plan, you have to enter a SIP address for the user. The address must be in the correct format, such as john.smith@company.com.
- If the user's UM mailbox policy is associated with an E.164 dial plan, you have to enter an E.164 address for the user. The address must be in the correct E.164 format, such as +14275551234. If the user's UM mailbox policy is associated with a SIP URI dial plan, you have to enter a SIP address for the user. The address must be in the correct format, such as john.smith@company.com.
- This option also requires that you manually enter a mailbox extension for the user. This extension number is used when the user accesses the mailbox via Outlook Voice Access. The number of digits in the extension number must match the number of digits configured on the dial plan for the user's UM mailbox policy.
- This option also requires that you manually enter a mailbox extension for the user. This extension number is used when the user accesses the mailbox via Outlook Voice Access. The number of digits in the extension number must match the number of digits configured on the dial plan for the user's UM mailbox policy.

7. Do one of the following, depending on whether you are using the Active Roles console or Web Interface:

- In the Active Roles console, click **Next** and wait while Active Roles performs the task. Then, click **Finish** to complete the wizard.
- In the Web Interface, click **Finish** and wait while Active Roles performs the task.

After you have enabled a user for Unified Messaging (UM), you may also want to view or change the UM-related properties of that user. For instructions, see [View or change the properties of a UM-enabled user](#) later in this document.

View or change the properties of a UM-enabled user

You can use Active Roles to view or configure the Unified Messaging (UM) properties of a user who is enabled for Unified Messaging. When you change a user's UM properties, you can control the user's access to various UM features. For example, you can enable or disable Automatic Speech Recognition (ASR) or fax receiving.

To view or change the UM properties of a UM-enabled user

1. Do one of the following, depending on whether you are using the Active Roles console or Web Interface:
 - a. In the Active Roles console,
 - i. Right-click the user, and then click **Properties**;
 - ii. In the **Properties** dialog box, click the **Mailbox Features** tab;
 - iii. On the **Mailbox Features** tab, click **Unified Messaging**, and then click **Properties**.
 - b. In the Web Interface,
 - i. Click the user, and then click the **Exchange Properties** command;
 - ii. On the **Exchange Properties** page, click the **Mailbox Features** tab;
 - iii. On the **Mailbox Features** tab, click **Unified Messaging**, and then click **Properties**.
2. Use the **Unified Messaging Properties** dialog box to view or change the following properties of the UM-enabled user:
 - **UM Mailbox Status** This area shows the Unified Messaging (UM) lockout status of the user's mailbox. Normally, the status is listed as **Not locked out**. The status of **Locked Out** indicates that the user is locked out of Unified Messaging due to a number of attempts to enter an incorrect Unified Messaging PIN in Outlook Voice Access.
 - **Unified Messaging mailbox policy** This field shows the name of the Unified Messaging mailbox policy associated with the UM-enabled user.
 - **UM extensions** This box displays the extension number and the Session Initiation Protocol (SIP) or E.164 address that are assigned to the UM-enabled user. The contents of this box depends upon the dial plan of the user's Unified Messaging mailbox policy. With a Telephone Extension dial plan, only the extension number configured for the user appears in this box. With a SIP dial plan, the extension number and SIP address are listed. With an E.164 dial plan, the extension number and E.164 address are listed.
 - **Enable for Automatic Speech Recognition** When selected, this option indicates that the UM-enabled user can access the mailbox by means of Automatic Speech Recognition (ASR). This option is selected by default, which allows the user to use voice commands when accessing the mailbox via Outlook

Voice Access. Even if enabled for ASR, the user must still use the keypad to enter the extension number and PIN.

- **Allow UM calls from non-users** When selected, this option allows incoming calls from unauthenticated callers through an auto attendant to be transferred to the UM-enabled user. By default, this option is selected, allowing callers from outside your organization to be transferred to the user inside the organization.

If this option is not selected, then an external caller who tries to transfer to the user receives the following response from the UM system: "I'm sorry, I am unable to transfer the call to this user." The caller is then transferred to the operator configured on the auto attendant.

This option does not affect callers who have signed in to their mailbox using Outlook Voice Access and are sending a voice message to the user.

- **Allow the user to receive faxes** When selected, this option allows the UM-enabled user to receive incoming faxes. By default, this option is selected. Unselect it if you do not want the user to receive incoming faxes.

This option is also configured on UM dial plans. If you select this option for a UM-enabled user, but the dial plan is configured to disallow fax receiving, the UM-enabled user is unable to receive faxes.

- **Allow diverted calls without a caller ID to leave a message** When selected, this option indicates that, for diverted calls without a caller ID, the caller is allowed to leave a message in the user's mailbox. By default, this option is selected, which makes it possible for the UM-enabled user to accept anonymous calls.
- **Allow users to configure call answering rules** When selected, this option allows the UM-enabled user to create personal auto attendants. This option is available to users with mailbox on a server running Exchange 2013 or later which does not hold the role of a Unified Messaging server. If this option is disabled on the UM dial plan or on the UM mailbox policy, it is not available to UM-enabled users associated with that UM mailbox policy.
- **Personal operator extension** Use this field to specify the operator extension number for the user. This enables incoming calls for the UM-enabled user to be forwarded to the extension number that you specify in this field. By default, an extension number is not configured. The range for the extension number is from 1 through 20 characters.

Other types of operator extensions can be configured on dial plans and auto attendants. However, those extensions are normally meant for company-wide receptionists or operators. The personal operator extension setting could be used when an administrative assistant or personal assistant answers incoming calls before they are answered by the user.

Reset Unified Messaging PIN for a UM-enabled user

When a UM-enabled user is locked out of the mailbox because of a number of attempts to enter an incorrect Unified Messaging PIN in Outlook Voice Access, or the user forgot the PIN, you can use Active Roles to reset the user's PIN. When you reset a user's PIN, you can configure Unified Messaging to automatically generate a PIN or you can manually specify the PIN. The new PIN is e-mailed to the user. If you prefer, you can specify additional PIN options when resetting the user's PIN.

To reset the Unified Messaging PIN for a UM-enabled user

1. Do one of the following, depending on whether you are using the Active Roles console or Web Interface:
 - In the Active Roles console,
 - a. Right-click the user, and then click **Exchange Tasks**;
 - b. Follow the steps in the Exchange Task wizard;
 - c. On the **Available Tasks** page, click **Reset Unified Messaging PIN**, and then click **Next**.
 - In the Web Interface, click the user, and then click the **Reset Unified Messaging PIN** command.
2. On the **Reset Unified Messaging PIN** page, complete the following fields:
 - **Automatically generate PIN to access Outlook Voice Access** Select this option to automatically generate a new PIN for the UM-enabled user. This is the default setting. If you select this option, a PIN is automatically generated based on the PIN policies configured on the user's UM mailbox policy. The automatically generated PIN will be sent in an e-mail message to the user's mailbox.
 - **Manually specify PIN** Select this option to manually specify a new PIN for the UM-enabled user. The PIN you specify with this option will be sent in an e-mail message to the user's mailbox.

The PIN must comply with the PIN policies configured on the user's UM mailbox policy. For example, if the UM mailbox policy is configured to accept only PINs that contain five or more digits, you must specify a PIN at least five digits long.

- **Require user to reset PIN on first telephone logon** Select this check box to force the user to reset the Unified Messaging PIN the first time that the user accesses the Unified Messaging system from a telephone.

It is a security best practice to force UM-enabled users to change their PIN upon their first logon to help protect against unauthorized access to their mailbox data. This is the default setting.

- **Require user to reset PIN at first logon** Select this check box to force the user to change the Unified Messaging PIN the first time that the user accesses

the Unified Messaging system from a telephone after you reset the PIN. It is a security best practice to force UM-enabled users to change their PIN upon their first logon to help protect against unauthorized access to their mailbox data.

3. Do one of the following, depending on whether you are using the Active Roles console or Web Interface:
 - In the Active Roles console, click **Next** and wait while Active Roles performs the task. Then, click **Finish** to complete the wizard.
 - In the Web Interface, click **Finish** and wait while Active Roles performs the task.

Disable Unified Messaging for a user

When you disable Unified Messaging (UM) for a UM-enabled user, the user is no longer able to use the UM features found in Microsoft Exchange Server. The user's UM settings are preserved after Unified Messaging is disabled for that user, so you can later re-enable the user for Unified Messaging and have the user's UM settings be the same as they were when Unified Messaging was disabled.

To disable Unified Messaging for a user by using the Active Roles console

1. Right-click the user, and then click **Exchange Tasks**.
2. Follow the steps in the Exchange Task wizard.
3. On the **Available Tasks** page in the Exchange Task wizard, click **Disable Unified Messaging**, and then click **Next**.

If the user is not enabled for Unified Messaging, the **Disable Unified Messaging** task does not appear on the **Available Tasks** page.

4. On the **Disable Unified Messaging** page in the Exchange Task wizard, click **Next** to confirm that you want to disable Unified Messaging for the user.
5. Wait while Active Roles performs the task.
6. Click **Finish** to complete the wizard.

You can also disable Unified Messaging for a UM-enabled user by using the Web Interface. To do so, click the user, and then click the **Disable Unified Messaging** command. As with the Exchange Task wizard, the **Disable Unified Messaging** command is not available unless the user is enabled for Unified Messaging.

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx>.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product